Deloitte.

Prudential Standard CPS 230 Operational Risk Management

The Shift from Implementation to Assurance

March 2026

MAKING AN IMPACT THAT MATTERS since 1845

Now that APRA's Prudential Standard CPS 230 is live, regulated entities must transition from implementation to embedding assurance in business-as-usual.

APRA's Prudential Standard CPS 230 – Operational Risk Management (CPS 230 or Standard) commenced in July 2025[1], marking a pivotal transition in the regulatory landscape.

After years of preparation and implementation, regulated entities are now operating under the applicable requirements of the standard. The implementation phase involved identifying Critical Operations and Material Service Providers (MSPs), setting tolerance levels and uplifting business continuity plans and operational risk frameworks.

With operations shifting to business-as-usual (BAU), APRA expects regulated entities to focus on sustained and independent assurance over the effectiveness of their framework across operational risk management (ORM), business continuity management (BCM) and service provider management (SPM).

In turn, MSPs to APRA regulated entities must establish assurance programs to validate the robustness of processes and controls underpinning their services that support clients' Critical Operations.

Achieving this requires targeted assurance programs that validate control effectiveness, uplift maturity and align with the Financial Accountability Regime (FAR) expectations. This provides senior management and Boards with confidence that CPS 230 obligations are being met on an ongoing and sustainable basis.

Drawing on Deloitte's experience, **this publication outlines key considerations for Internal Audit** to provide robust and insightful assurance to financial service institutions (FSIs), **while also highlighting the implications for MSPs** in ensuring services are underpinned by strong controls and assurance, in line with APRA expectations.

[1]APRA has outlined a longer implementation timeline for specific CPS 230 requirements for Non-Significant Financial Institution's (SFI)s.

Integrated Assurance across the 'Three Lines of Defence'

1st Line

Ownership & Execution

- Identify, assess, and manage operational risks (including service provider risks).
- Design and operate internal controls to maintain Critical Operations within tolerance.

2nd Line

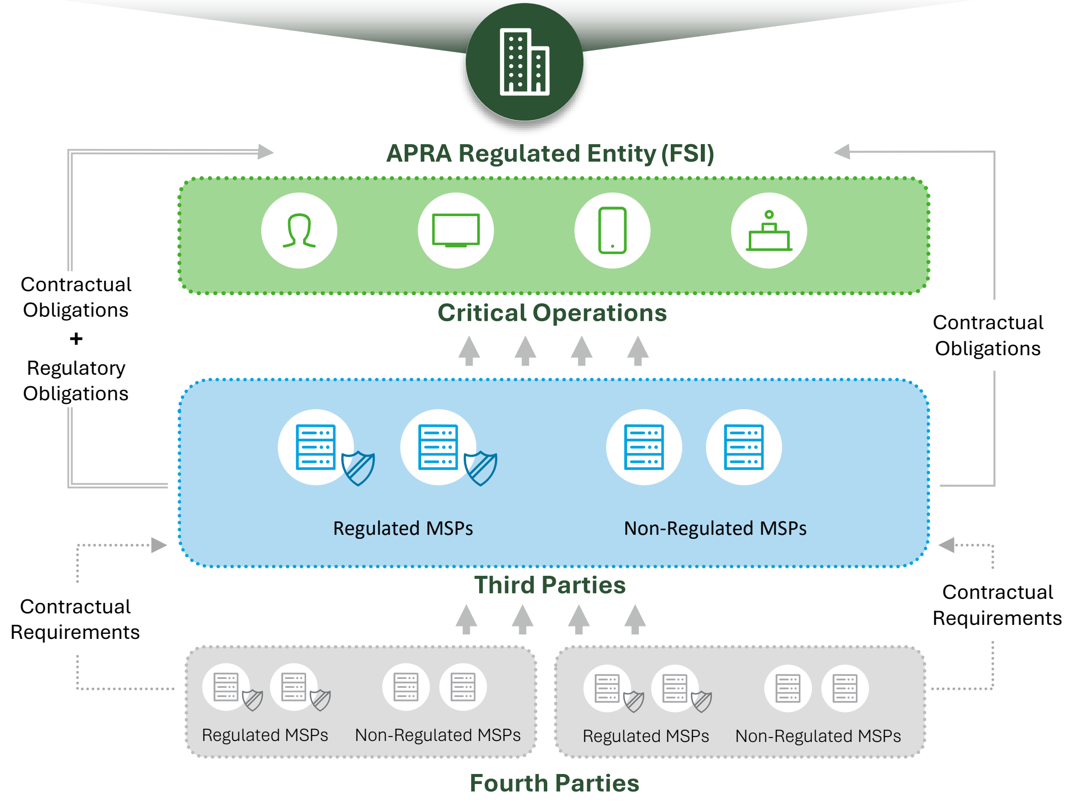
Oversight & Challenge:

- Develop the CPS 230 framework and supporting policies.
- Monitor risk profiles against tolerances and challenge the effectiveness of 1st Line controls.

3rd Line

Independent Assurance

- Provide the Board/Audit Committee with Independent Assurance on the design and operating effectiveness of the CPS 230 framework and supporting controls, including those related to MSPs.



Internal Audit has a key role to play under CPS 230, providing assurance that reaches beyond baseline compliance to a holistic view of resilience in relation to Critical Operations and third and fourth parties. Delivering on this requires a thoughtful and phased IA plan, starting with the mandatory requirements of the standard and progressively expanding into thematic deep-dive areas.

Mandatory IA Scope Area : *Review of the BCP (paragraph 46) [Year 1 – 2]*

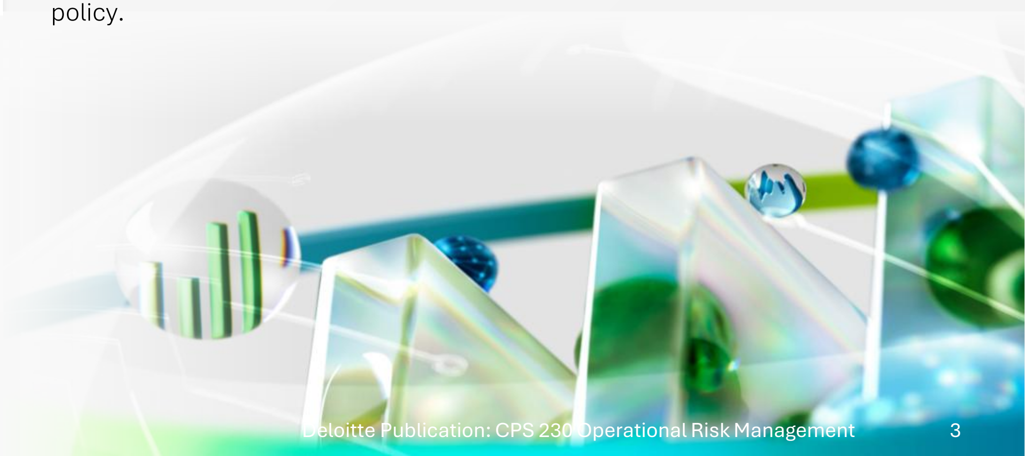
As required by CPS 230 paragraph 46, IA should review the organisation's BCP(s) to validate these plans are credible. In determining this, APRA would expect IA to review and assess:

1. **Structure and Format**: Completeness and relevancy of components and usability.
2. **Scope:** Critical Operations (and sub-component) coverage.
3. **Recovery Strategies and Contingency Arrangements:** Including data or testing limitations, execution risks, or assumptions associated with recovery strategies.
4. **MSPs:** Is the reliance on MSPs to support recovery of Critical Operations understood and reflected in contractual agreements and has it been tested? Do the MSPs have a clear understanding of who their key service providers are (fourth parties to APRA regulated entities) and these link into the client's ?
5. **Disaster Recovery:** Alignment of recovery time objectives (RTOs) with Tolerance Levels for critical systems supporting Critical Operations.
6. **Roles and responsibilities:** Are the roles a responsibilities required to support recovery / continuity clearly defined and in place?
7. **Supporting plans:** Integration of crisis management and communication plans, vendor-specific contingency plans, and scenario playbooks with the BCP
8. **Notification and Escalation:** Protocols for notifying and escalating potential disruptions, including activating and de-activating plans?
9. **Crisis communications:** Internal and external communications, including MSPs.
10. **Board endorsement:** Has the Board reviewed and endorsed the BCP, including all identified critical operations?

Mandatory IA Scope Area : *Review of Material Outsourcing Arrangements (paragraph 60) [Year 1 – 2]*

As required by CPS 230 paragraph 60, IA must review any proposed material arrangements involving the outsourcing of a critical operation.

It is acknowledged that the first year of CPS 230 is a transitional one as it relates to material arrangements, however, it is recommended that IA undertake a phased approach to reviewing such arrangements (both new / proposed and existing), as and when they are executed (a risk-based sample would be appropriate, depending on the number of MSPs). The review should be performed with reference to material arrangement requirements in CPS 234 paragraphs 54 to 56 inclusive, as well as the organisation's own service provider management policy. IA must also regularly report to the Board or Board Audit Committee on compliance of such arrangements with the entity's service provider management policy.



Recommended IA Scope Area: *Post-implementation Review [Year 1 – 2]*

In year 1 – 2, and as CPS 230 practices are embedded by the business, IA should undertake a post-implementation review and, at a minimum, start by focusing on the first three key areas as per APRA's CPS 230 compliance checklist – Critical Operations, Tolerance Levels and MSPs. Below and adjacent we have expanded on each of these and listed recommended IA focus areas for each:

Critical Operations:

- **Methodology:** Is there clearly defined criteria to assess the criticality of Business Operations in a consistent and robust manner?
- **Critical and Non-Critical Operations:** Is there a documented view of the organisation's Critical and Non-Critical Operations? Is the assessment of Critical and Non-Critical Operations reasonably justified by supporting metrics and data?
- **Risk Profiling:** Is there a clear understanding of the risks, controls and obligations associated with Critical Operations, and where there may be control gaps and vulnerabilities?
- **Accountability:** How are Critical Operation Owners meeting their accountabilities? How have Financial Accounting Regime (FAR) accountability statements been revised?
- **Monitoring:** Are there clear mechanisms for the ongoing monitoring of Critical Operations, including process for escalating and notifying potential disruptions impacting Critical Operations?
- **Management and Board Reporting:** Is there structured and timely reporting of status, risks, and performance of Critical Operations?

Tolerance Levels

- **Methodology:** Is there a clearly documented methodology to support setting of Tolerance Levels in a consistent and robust manner?
- **List of Tolerance Levels:** Have Tolerance Levels been clearly documented for each Critical Operation and approved by the Board? Are these well-defined and measurable?
- **Linkage between RAS and Tolerance Levels:** How are these linked?
- **Monitoring:** How are tolerance levels measured or monitored?

MSPs

- **Methodology:** Is there a clearly defined criteria to assess the materiality of Service Providers?
- **Process to understand and document risks, controls, monitoring and reporting:** Including RAS limits / metrics.
- **Concentration risks and Step-In risk:** Where are the concentration and / or step-in risks?
- **Tolerance Impact:** Consider the tolerance and limits of these parties when relied upon, including the timing of their testing and the level of visibility the entity has into these aspects.
- **Completeness and accuracy:** Are identified Service Providers complete and accurate? Are those that are identified as Material and Non-Material appropriate?
- **Fourth Parties:** How are fourth parties identified and managed?
- **Contracting:** How are Critical Operations and Tolerance Levels considered?

Recommended IA Scope Area: *Remediation Review [Year 1 – 2]*

As CPS 230 was being implemented, it is likely that regulated entities identified gaps against compliance with the standard (e.g., control gaps identified in risk profile for COs/MSPs or weaknesses at the back of BCP testing).

IA should consider reviewing such gaps and ensuring that they are being managed / tracked or risk accepted in accordance with relevant policies, and that there is clear ownership and a plan to remediate in a timely manner. IA should also ensure that the Board is being kept informed of progress against these plans, including delays to planned remediation dates.

Recommended IA Scope Area: *Systematic Testing Program [Year 2 – 3]*

Fundamentally, CPS 230 was introduced to ensure organisations are adequately prepared to sustain the delivery of Critical Operations during severe disruptions. Central to this objective is the credibility of BCPs which relies on robust and regular testing. Given IA's role in providing assurance over BCP effectiveness, a review of the organisation's Systematic Testing Program is required.

Where possible, IA should consider observing BCP tests to gain true insights into its execution (whilst remaining at arm's length and maintaining independence). IA should then ensure that testing results are formally documented and reported to the Board, and that findings are executed.

Ongoing Considerations

From years 2 to 3 onwards, as well as continuing to meet the mandatory compliance requirements outlined on page 3 (on a cyclical basis as required), IA has an opportunity to add further value through carefully curated, resiliency-focused reviews. Examples include:

- **MSP exit planning and termination:** Assess whether exit strategies and termination arrangements for MSPs are defined and operationalised to support continuity of Critical Operations and compliance with CPS 230.
- **Fourth party management:** Evaluate the effectiveness of controls to identify, assess and manage fourth-party risks, including visibility of critical dependencies and contractual protections supporting CPS 230 resilience requirements.
- **Operational Risk Management Framework (ORMF) integration with risk appetite and KRIs:** Review the alignment of the ORMF with Board-approved risk appetite and KRIs, including how operational risk exposures and tolerances are monitored and escalated.
- **Extended enterprises interlinkages:** Assess how risks arising from extended enterprise interdependencies (including intra-group, outsourcing and technology ecosystems) are identified, managed and aggregated to support end-to-end operational resilience under CPS 230.
- **Culture and accountability (cross-cutting audit):** Assess how CPS 230 has influenced operational risk culture and accountability frameworks, including technology and operational resiliency by design.
- **Management information:** IA functions should continue to apply challenge to the quality and effectiveness of MI to ensure it is – and continues to be, in light of business change - appropriate for business needs. For example, IA should challenge management on the use of data-driven insights to identify emerging risks and trends, using key risk indicators (KRIs) and key performance indicators (KPIs) to monitor operational resilience, and encourage the move beyond reactive reporting to proactive insights on emerging risks and opportunities.

Based on the insights from this and the previous page, **below we have drafted an indicative IA plan**. Whilst IA planning is not one-size-fits-all and will depend upon the size and nature of an organisation, the below acts as an example of how IA can contribute, not only to CPS 230 compliance, but also to the broader resiliency of the enterprise.

Year 1	Post-implementation Review	Remediation Review	***Review of BCP(s)***	***Review of Material Outsourcing Arrangements*** (phased)
Year 2	Review / Observation of Systematic BCP Testing Program	Review of Ongoing MSP Oversight / Due Diligence		
Year 3 Onwards	MSP Exit Planning & Termination Review	Fourth Party Management Review	Review of ORMF Integration with Risk Appetite & KRIs	Extended Enterprises Interlinkages
	Culture & Accountability Review		Management Information Review	

Legend: ***Mandatory Requirement***

CPS 230 Assurance is as vital for **Material Service Providers (MSPs)** as it is for the financial services industry.

Robust CPS 230 assurance is as vital for MSPs as it is for the financial services industry. It reinforces MSP processes and controls that sustain critical FSI operations, while promoting transparency and confidence.

The design of an MSP assurance program must begin with a clear understanding of the linkages and interdependencies between MSPs and FSIs. This understanding would help define MSP assurance objectives and determine a phased / risk-based approach to program execution.

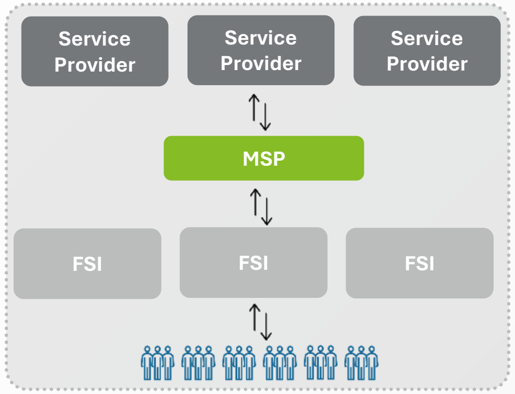
A practical and efficient model for MSPs to obtain this assurance is to use a 'Third-party Assurance' (TPA) report.

A TPA report, issued under a formal assurance standard (e.g., ASAE 3150), would offer benefits to MSPs and FSIs (as users):

- MSPs can use TPA reports to meet assurance requirements of both internal (management / Board) as well as external (FSIs) stakeholders.
- One TPA report accepted by multiple FSIs allows MSPs to save time and resources and prevents the need for multiple audits.
- FSIs can compare multiple MSPs in a structured and consistent way. This simplifies overall service-provider management and governance.

Understanding FSI-MSP linkages

FSIs and MSPs must collaboratively understand how MSP functions fit into FSI critical operations. **This alignment would ensure MSPs have the capacity and the commitment to meet minimum service levels (thresholds)** for operational resilience and service continuity.



FSI Lens – Identifying implications for MSPs

Under CPS 230, FSIs identify Critical Operations which, if disrupted beyond set tolerances, would materially impact customers. Where these operations rely on third parties—or where third-party arrangements are deemed material—they are classified as MSPs.

As a result, FSIs must be confident about the reliability and robustness of MSP operations and underlying controls.

MSP Lens – Translating FSI requirements into MSP assurance outputs

Recognising expectations of CPS 230 and FSI requirements, what are the implications for MSPs?

- Clearly understand which services are being provided to FSIs and how they support Critical Operations.
- Establish a transparent process to identify indirectly impacted services and manage customer engagement with Risk and Legal.
- Create a standard contracting playbook with pre-defined clauses, fallback positions, and non-negotiables.
- Understand resources and interdependencies to identify vulnerabilities and strengthen controls, testing, and response.
- Ensure the right teams are accountable and processes align with regulatory expectations to support a repeatable compliance model.

Business Continuity Management

- Recovery of critical operations must be embedded in BCPs.
- Tolerances must be aligned with MSP customers.
- BCP test strategy must incorporate scenario testing and testing upstream supplier dependencies.

Service Provider Management

- Identify and uplift supplier risk management and contingency planning.
- Identify contract clauses for suppliers and plan for contract uplift requests from entities.
- When supporting Critical Operations for multiple entities, establish common libraries of communication protocols, FAQs and recovery playbooks.

Operational Risk Management

- Mapping processes and resources supporting Critical Operations.
- Defining triggers for incidents, breaches and alerts to entities.
- Ongoing testing of controls to maintain design and operating effectiveness.

Contact

Puneet Gulati

Partner

pugulati@deloitte.com.au

M: +61 (0)447 523 911

Aneleise Algie

Partner

amaione@deloitte.com.au

M: +61 (0)437 266 393

Kerrie-Ann Rodrigues Barrett

Partner

kerbarrett@deloitte.com.au

+61 (0)421 832 303

Tarah Unn

Director

tunn@deloitte.com.au

M: +61 (0)416 775 623

Deloitte.