CPG 230 Operational Risk Management

Final Guidance
June 2024

On 13 June 2024, APRA formally released its final Prudential Practice Guide CPG 230 Operational Risk Management.

Summary of key changes

In response to consultation feedback received from 16 entities and industry bodies, APRA recognised the requirement for greater clarity to avoid the creation of unintentional practical difficulties during implementation. The guidance has been simplified to be shorter, sharper and focused on effective baseline compliance. Whilst maintaining strong expectations around achieving resilience, APRA has effectively given regulated entities more flexibility around how they achieve stronger resilience outcomes by applying more of a risk-based lens to their approaches. Key changes include:

- **Day One checklist** – entities should consider the summary of requirements and suggested order of implementation in their plans.
- **Non-Significant Financial Institutions** have an additional 12 months to comply with certain requirements in CPS 230 relating to business continuity and scenario analysis.
- **A three-year forward plan** has been provided on APRA's intended approach to supervising CPS 230 to assist industry with implementation and planning.

Key changes per section

Roles and Responsibilities

- Less prescriptive guidance as to how the Board delegates responsibility to senior management, providing more flexibility to entities in application. Noting, however, that processes for delegation between the Board and Senior Management should be clear and documented.
- Entities should consider how delegated responsibilities align to accountability for Operational Risk Management under FAR.
- Less prescriptive on what effective oversight by the Board entails.

Operational Risk Management

- Promotion of Critical Operations as the key focal point for operational risk management practices and procedures, including risk profiling.
- Less prescriptive guidance and expectations on the approach for end-to-end process and resource mapping, providing more flexibility to Senior Management in implementation.
- Removal of detailed guidance on approach to maintaining operational risk profiles, including risk identification and assessment, control management and testing, incident management and root cause analysis. Replaced with high-level considerations.

Business Continuity

- Less prescriptive guidance, with the removal of better practice statements, regarding:
  - approach to Business continuity management;
  - detail of BCPs and alignment to disaster recovery;
  - BCP testing approach.
- Addition of MSP details to Critical Operations register.
- Removal of indicative/relative tolerance levels.
- Removal of sound practice for tolerance of data loss

Material Service Providers

- Guidance provided on attributes to be included in the MSP register, specifying attributes not previously requiring disclosure (e.g. responsible persons, mapping to Critical Operations and/or material operational risks, list of fourth parties, etc.). In Q3 2024, APRA will provide a template register.
- APRA requests that for SFIs, the first MSP register is to be submitted by 1 October 2025.

- Clarification that service providers within a material cohort are not required to be classified as material as long as they are not individually material.
- Clarification that arm's length transactions with the prescribed list of service providers does not result in a material arrangement. Material arrangements arise only when there is reliance on a critical operation or exposure to a material operational risk.
- Guidance on the need for Internal Audit to review any proposed outsourcing of critical operations prior to a decision being made and the capability and capacity to do so.
- Removal or less prescriptive guidance relating to the following, allowing more flexibility for the depth to which entities can take:
  - the identification and assessment of downstream service providers;
  - provisions within service agreements;
  - approach to monitoring performance.

Implementation considerations

- **Critical Operations Mapping** – Determine the level of process and resource mapping that is of sufficient detail for senior management to understand how Critical Operations are delivered during business-as-usual and maintained during disruption.
- **Material Service Providers (MSP)** – Consideration of the operational risks of cohorts of service providers where the aggregate risk is material in addition to MSPs.
- **Fourth Parties** – Determine the approach to identifying fourth parties supporting MSPs and the impact they could have on the critical operation.

Key focus areas

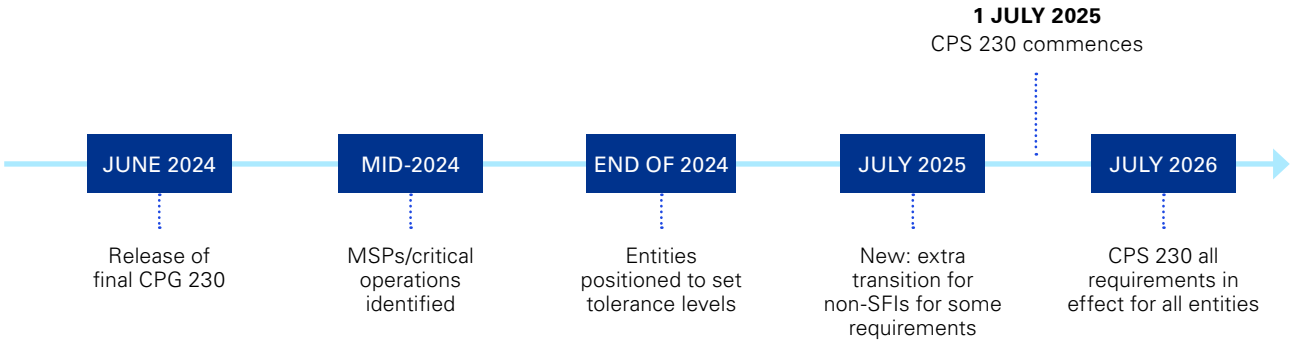
Over and above the extensive work completed by clients to this point, KPMG is focusing its support in the following key areas:

- Mapping **processes, risks and controls for critical operations.**
- **Support for defining** vulnerabilities, **severe but plausible scenarios** and a **testing library.**
- Conducting **pre-implementation or readiness assessments.**
- Supporting definition of an **operating model** that **articulates clear accountability** across business divisions, central functions (BCM, Supplier Management, Technology), senior management and Board.
- Accelerating Material Service Provider assessments through **finalisation of enhanced frameworks**, but also providing capability and capacity to **accelerate the program of conducting the MSP assessments.**
- Defining and implementing a program of responding to information requests and risk assessments **for those entities that are also Material Service Providers** to other regulated entities.

"By amending the accompanying guidance, we aim to keep industry standards high while also being mindful of the compliance burden on smaller entities so they can remain competitive."

JOHN LONSDALE, APRA CHAIR

IMPLEMENTATION TIMELINE



Appendix A: CPS 230 compliance checklist

REQUIREMENT	SUBMISSION TO APRA	UPDATED OR NEW REQUIREMENT
1. Critical Operations (COs) are identified.	Entities are not required to submit their list of critical operations. However, an APRA supervisor could request it.	NEW as concept of critical operations is introduced by CPS 230.
2. Tolerances are defined and approved by the Board for COs (time, data loss, and service level).	Entities are not required to submit tolerance lists. However, an APRA supervisor could request it, to understand how critical operations are monitored and to confirm Board approval as required by the Standard.	UPDATE as tolerances exist under CPS 232 for time and SLAs. CPS 230 applies a Critical Operations lens.
3. Material Service Providers (MSPs) are identified.	Entities are required to submit a register of MSPs to APRA on an annual basis. APRA requests the first submission by 1 Oct 2025. This is the key data requirement of CPS 230 along with incident notifications and supplier/ offshore notifications.	NEW but building on the requirements that have been in place under CPS 231, in monitoring and oversight of suppliers.
4. Notifications are operational for material events, tolerance breaches and MSP changes.	Entities are required to have notifications to APRA in place per paragraphs 33 (material events), 49 (tolerance breach) and 59 (MSP arrangement/offshoring changes).	UPDATE as notification requirements do exist under CPS 231 and CPS 232 in the current architecture.
5. Board Governance & Oversight is in place and clear roles and responsibilities are set.	Entities are not required to submit updated senior management accountabilities or target operating model documentation. This could be requested and discussed as part of a prudential review.	UPDATE to align with the critical operations requirements in CPS 230 but builds on CPS 220 positioning.
6. Risk Profiles & Reporting is established and supporting oversight accountabilities.	Entities are not required to submit risk profiles or risk reporting as part of compliance with CPS 230. These could be requested and discussed as part of a prudential review.	UPDATE against critical operations and building on CPS 220, 231, 232 foundations.
7. Accountability for COs, MSPs, and monitoring is in place.	Entities are not required to submit updated operational accountabilities or examples of BAU monitoring, reporting or controls for compliance with CPS 230. These could be requested as part of a prudential review.	UPDATE to accountabilities, to refer to new concepts introduced under CPS 230 building on CPS 220, 231, 232 foundations.
8. Contract Updates have an extension of 12 months per paragraph 7 of the standard.	Entities have an additional 12 months to ensure that pre-existing service provider arrangements comply with contract requirements under CPS 230.	UPDATE to pre-existing contracts to comply with CPS 230.
9. Business Continuity Management (BCM) shifts from Critical Operations focus.	Entities are not required to submit their updated BCM strategy, policy, or plans. These could be requested and discussed as part of a prudential review.	UPDATE of existing BCM policy, plans, testing under CPS 232 to the CPS 230 Critical Operations focus.
10. Scenarios align with BCM uplift and focus on severe yet plausible scenarios for Critical Operations and Material Service Providers.	Entities are not required to submit their new scenarios or testing results as part of CPS 230 compliance. This could be requested and discussed as part of a prudential review.	UPDATE of existing scenario approach under CPS 232 to apply a CPS 230 Critical Operations lens.

Appendix B: Transition details for non-SFIs

CPS 230: REQUIREMENTS THAT WILL NOW COMMENCE 1 JULY 2026 FOR NON-SFIs (PREVIOUSLY 1 JULY 2025)	
40.	An APRA-regulated entity's BCP must include: – the register of critical operations and associated tolerance levels; – triggers to identify a disruption and prompt activation of the plan, and arrangements to direct resources in the event of activation; – actions it would take to maintain its critical operations within tolerance levels through disruptions; – an assessment of the execution risks, required resources, preparatory measures, including key internal and external dependencies needed to support the effective implementation of the BCP actions; and – a communications strategy to support execution of the plan
41.	An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology. An APRA-regulated entity must monitor compliance with its tolerance levels and report any failure to meet tolerance levels, together with a remediation plan, to the Board.
43.	An APRA-regulated entity must have a systematic testing program for its BCP that covers all critical operations and includes an annual business continuity exercise. The program must test the effectiveness of the entity's BCP and its ability to meet tolerance levels in a range of severe but plausible scenarios.
44.	The testing program must be tailored to the material risks of the APRA-regulated entity and include a range of severe but plausible scenarios, including disruptions to services provided by material service providers and scenarios where contingency arrangements are required. APRA may require the inclusion of an APRA-determined scenario in a business continuity exercise for an APRA-regulated entity, or a class of APRA-regulated entities.
45.	An APRA-regulated entity must update, as necessary, its BCP on an annual basis to reflect any changes in legal or organisational structure, business mix, strategy or risk profile or for shortcomings identified as a result of the review and testing of the BCP.
46.	An APRA-regulated entity's internal audit function must periodically review the entity's BCP and provide assurance to the Board that the BCP sets out a credible plan for how the entity would maintain its critical operations within tolerance levels through severe disruptions and that testing procedures are adequate and have been conducted satisfactorily.

CPS 232: REQUIREMENTS THAT CONTINUE UNTIL 30 JUNE 2026 FOR NON-SFIs	
30.	An APRA-regulated institution must maintain at all times a documented BCP for the institution that meets the objectives of the institution's BCM policy.
31.	The BCP must document procedures and information that enable the institution to: – manage an initial business disruption (crisis management); and – recover critical business operations.
32.	The BCP must reflect the specific requirements of the institution and must identify: – critical business operations; – recovery levels and time targets for each critical business operation; – recovery strategies for each critical business operation; – infrastructure and resources required to implement the BCP; – roles, responsibilities and authorities to act in relation to the BCP; and – communication plans with staff and external stakeholders.
33.	Where material business activities are outsourced, an APRA-regulated institution must satisfy itself as to the adequacy of the outsourced service provider's BCP and must consider any dependencies between the two BCPs.
34.	An APRA-regulated institution must review and test the institution's BCP at least annually, or more frequently if there are material changes to business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.
35.	The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 34.

Appendix B: Transition details for non-SFIs

SPS 232: REQUIREMENTS THAT CONTINUE UNTIL 30 JUNE 2026 FOR NON-SFIs	
21.	An RSE licensee must maintain at all times a documented BCP that meets the objectives of the BCM Policy.
22.	An RSE licensee's BCP must document procedures and information that enable the RSE licensee to: – manage an initial business disruption (crisis management); and – recover critical business activities.
23.	An RSE licensee's BCP must reflect the specific requirements of the RSE licensee and must identify: – critical business activities; – recovery levels and recovery times for each critical business activity; – recovery strategies for each critical business activity; – infrastructure and resources required to implement the BCP; – roles, responsibilities and authorities to act in relation to the BCP; and – communication plans with staff and external stakeholders.
24.	Where material business activities are outsourced, an RSE licensee must satisfy itself as to the adequacy of the outsourced service provider's BCP and must consider any dependencies between the two BCPs.
25.	An RSE licensee must review and test its BCP at least annually, or more frequently if there are material changes to its business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.
26.	The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 25.

Contact us

Matt Tottenham
Partner in Charge, Regulatory & Compliance
T: +61 436 188 811
E: mtottenham@kpmg.com.au

Gavin Rosettenstein
Partner, Operational & Service Provider Risk Management
T: +61 413 956 179
E: gavin1@kpmg.com.au

Kat Conner
Partner, Risk Transformation, Regulatory & Compliance
T: +61 438 057 483
E: katconner@kpmg.com.au

Natasha Passley
Partner, Business Continuity & Operational Resilience
T: +61 411 010 209
E: npassley@kpmg.com.au

Caroline Leong
Partner, Process Architecture and Modelling
T: +61 423 030 794
E: cleong1@kpmg.com.au

Dr Lisa Butler Beatty
Partner and Practice Lead, Superannuation Advisory
T: +61 477 753 941
E: lisabbeatty@kpmg.com.au

Louise Rose
Partner, Enterprise Advisory
T: +61 478 159 379
E: lrose2@kpmg.com.au

Fiona Jarmson
Director, Regulatory & Compliance
T: +61 438 688 155
E: fjarmson@kpmg.com.au

Simon Taylor-Allan
Director, Operational Risk Management
T: +61 427 962 177
E: staylorallan@kpmg.com.au

KPMG.com.au

June, 2024. 1378250952FS.