Article Information

Authors: Lisa-Marie McKechnie, Kathy Neilson, Kerry Jacobs, Wendy Gao
Service: Corporate & Commercial, Corporate Governance
Sector: Financial Services

APRA releases final version of new operational risk management prudential standard CPS 230

After many months of consultation by APRA on the previous draft (released in July 2022), APRA has now released the final version of CPS 230, the new prudential standard on operational risk management. We delve into what this means for banks, insurers, superannuation trustees and other APRA-regulated entities.

The Australian Prudential Regulation Authority (**APRA**) released the final version of cross-industry Prudential Standard CPS 230 Operational Risk Management (**CPS 230**) on 18 July 2023. The aim of this new standard is to ensure that APRA-regulated entities can effectively address and manage operational risk, particularly in relation to their critical operations and material service providers. The release follows an extensive period of consultation with industry on a draft version of CPS 230 released in July 2022 and a period of consideration of submissions by APRA. In addition, APRA has also released a draft Prudential Practice Guide CPG 230 Operational Risk Management (**CPG 230**) for consultation with submissions closing on 13 October 2023.

CPS 230 replaces and supersedes five existing prudential standards and five existing prudential practice guides relating to outsourcing and business continuity management, streamlining the risk management supporting standards to maintain effective risk management strategies and systems.

The finalised CPS 230, which will commence from 1 July 2025, imposes the burden of responsibility on regulated entities to be proactive in fulfilling its obligations under the new standard. The Board is ultimately accountable for the oversight of the APRA-regulated entity's operational risk framework, including ensuring its continued resilience in the face of operational risks and business disruptions and also the management of service provider arrangements. In addition, the Board must ensure senior managers within an APRA-regulated entity are set clear roles and responsibilities for operational risk management, including business continuity and management of service provider arrangements. These changes represent an important step in the path towards preserving and enhancing a stable and resilient financial services industry.

New changes in the final CPS 230

The main changes between the draft CPS 230 and the finalised CPS 230 are as follows:

- The new standard now commences on 1 July 2025 instead of 1 January 2024. Where an APRA-regulated entity has pre-existing contractual arrangements in place with a service provider, the requirements in CPS 230 will apply in relation to those arrangements from the earlier of the next renewal date of the contract or 1 July 2026 (whichever is earlier);
- In the assessment of an APRA-regulated entity's operational risk profile, a defined risk appetite must now also be supported by tolerance levels in addition to indicators and limits;
- Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's recovery and exit planning (previously, there was to be no conflict with an APRA-regulated entity's financial contingency planning);
- While an APRA-regulated entity must manage its full range of operational risks, reputational risk is no longer included as part of this non-exhaustive list of operational risks;
- Appropriate and sound information and information technology (IT) capability must be maintained (previously, reference was made only to IT infrastructure);

- An APRA-regulated entity must monitor the age and health of its information assets (previously, reference was made only to IT infrastructure);
- There has been clarification made to functions that are deemed by APRA to be critical operations in relation to certain types of APRA-regulated entity. In addition, an APRA-regulated entity must, at a minimum, classify certain business operations as critical operations, unless it can justify otherwise. These deemed critical operations include:
    - For an ADI: payments, deposit-taking and management, custody, settlements and clearing;
    - For an insurer (general, life, private health): claims processing;
    - For an RSE licensee: investment management and fund administration; and
    - For all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations;
- Tolerance levels for each critical operation of an APRA-regulated entity now do not require Board approval;
- If there has been a disruption to a critical operation outside tolerance, an APRA-regulated entity must notify APRA as soon as possible and not later than 24 hours after the disruption;
- The comprehensive service provider management policy:
    - no longer needs to include a register of the entity's material service providers; and
    - must now include the entity's approach to managing risks associated with any fourth parties that material service providers rely on to deliver a critical operation to the APRA-regulated entity;
- Material arrangements are now defined to be those on which the entity relies to undertake a critical operation or that expose it to material operational risk;
- The following providers that provide such services are now classified as a material service provider (unless the APRA-regulated entity can justify otherwise):
    - For an ADI: credit assessment, funding and liquidity management, and mortgage brokerage;
    - for an insurer (general, life, private health): underwriting, claims management, insurance brokerage, and reinsurance;
    - for an RSE licensee: fund administration, custodial services, investment management and arrangements with promoters and financial planners; and
    - for all APRA-regulated entities: risk management, core technology services and internal audit.
- APRA may now declare any service provider arrangement as material (in addition to the ability to declare a service provider to be material). Further the requirement to undertake a tender process in relation to the material arrangement has been removed however an appropriate selection process and an assessment of the ability of the service provider to provide the service on an ongoing basis remains as requirement;
- An APRA-regulated entity no longer needs to take reasonable steps to assess whether a service provider is systemically important in Australia when entering into or material modifying a material arrangement;
- In addition to the enhanced contractual content requirements that appeared in the draft version of CPS 230, for all material arrangements, the agreement must require notification by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through sub-contracting or other arrangements;
- An APRA-regulated entity's internal audit function must review any proposed material arrangement involving the outsourcing of a critical operation. The internal audit function must also regularly report to the Board on compliance of material arrangements with the entity's service provider management policy.

Key Take Aways for APRA-regulated entities

The Boards and senior management of APRA-regulated entities must have a clear understanding and be proactive in reassessing, reviewing and improving their entities' operational risk framework. Even though APRA has extended the timeframe for compliance, given the number of new requirements and the cross-organisational impact, APRA-regulated entities should take action now by:

- Identifying the APRA-regulated entity's critical operations, material service providers (both external and internal) and material arrangements;
- Reviewing external and internal service provider arrangements to ensure compliance with the enhanced contractual content requirements in CPS 230 and documentation of any undocumented internal service provider arrangements will be achieved by the relevant commencement date;
- Conducting reviews, of all existing operational risk and business continuity policies and procedures to ensure compliance with CPS 230;
- Identifying any weaknesses in existing operational risk frameworks and implementing more comprehensive compliance initiatives if necessary;
- Conducting training for all Board members, risk management teams and other stakeholders to ensure adequate understanding of each party's responsibilities and roles in addressing and implementing the new standard;
- Documenting and implementing new policies, procedures, charters and protocols to ensure compliance with CPS 230 including in relation to the required service provider management policy and required board and senior management roles and reporting;

- Review the draft guidance in CPG 230 and consider providing feedback to APRA by the consultation deadline of 13 October 2023.