HERBERT SMITH FREEHILLS

AUSTRALIAN REGULATOR CONSULTS ON NEW OPERATIONAL RISK MANAGEMENT PRUDENTIAL STANDARD

05 August 2022 | Australia
Legal Briefings – By **Peter Jones, Katherine Gregor, Andrew Bradley, Maged Girgis, Charlotte Henry and Rebecca Gill**

The Australian Prudential Regulation Authority (**APRA**) has released its consultation on a new cross-industry prudential standard for operational risk management, CPS 230, which proposes to introduce a range of new requirements on APRA-regulated entities for managing operational risk and enhance existing requirements for business continuity and service provider management

A SNAPSHOT

Operational resilience is critical to the stability of financial institutions and has been an area of increasing focus for APRA in recent years. The Coronavirus pandemic has proven to be a real-world test of the operational resilience of APRA-regulated entities and has rapidly escalated the pace of change in the way organisations do business. At the same time, APRA-regulated entities have had to manage a broad and multi-faceted range of operational risks, ranging from disruptions to supply chains, increasing cybersecurity risks and risks arising from geopolitical and economic uncertainty. Against this backdrop, on 28 July 2022, APRA released a discussion paper and began consultation on draft prudential standard CPS 230.

Draft CPS 230 introduces new and enhanced requirements to strengthen the operational resilience of APRA-regulated entities and improve how those entities manage operational risk. It also consolidates and enhances existing standards in relation to third-party risk management, outsourcing and business continuity by replacing a number of existing prudential standards (CPS/SPS/HPS 231 and CPS/SPS 232). CPS 230 will apply to all APRA-regulated entities, including banks, insurers (general, life and health) and registrable superannuation entity licensees.

In developing draft CPS 230, APRA has adopted a principles-based approach which is designed to focus on outcomes rather than process. While this approach will be familiar to APRA-regulated entities and is consistent with APRA's current approach to prudential regulation of operational risk management, the proposal to consolidate a number of existing prudential standards means that in some respects CPS 230 is even less detailed (and therefore less prescriptive) than the predecessor standards it will replace. This raises difficult questions about the extent to which the predecessor standards remain instructive and the extent to which APRA will rely on guidance to inform its policy position and its expectations of APRA-regulated entities.

While CPS 230 is less prescriptive in some respects, it does introduce a range of new and enhanced requirements that APRA-regulated entities will need to comply with and also bestows significant additional powers on APRA.

APRA is inviting submissions to the consultation on draft CPS 230 by 21 October 2022, with the prudential standard expected to come into effect on 1 January 2024.

KEY TAKEAWAYS

- Draft CPS 230 proposes a number of enhanced obligations on APRA-regulated entities, such as an express obligation to 'effectively manage' operational risk and, to the extent practicable, 'prevent disruption to critical operations'.

- Draft CPS 230 uses more onerous language in describing the roles and responsibilities of the Board and senior management – for example, rather than saying the Board is 'responsible' for oversight of risk management the revised standard refers to the Board as 'accountable' for oversight of risk management. The standard also increases the level of accountability of senior managers within the organisation.

- APRA is giving itself a number of significant additional powers, including to require the entity to hold additional capital, impose conditions on the entity's licence, independent review and remediation if APRA considers that an entity's operational risk management has material weaknesses.

- Requirements for services provided by third parties are proposed to significantly expand, moving from the existing focus in CPS 231 (and equivalents) on 'outsourcing' material

business activities to a broader concept of ‘material service providers’. This change in terminology will likely capture a broader range of third parties and require a register of material service providers to be maintained and provided to APRA annually.

- New requirements in respect of managing ‘fourth parties’ (being any party that a service provider relies on in delivering services to an APRA-regulated entity) have been proposed, such that an entity’s service provider management policy must address the entity’s approach to managing risks associated with any ‘fourth parties’ and contracts with material service providers must require notification by the service provider of its use of other material service providers (e.g. through sub-contracting or other arrangements). It appears that the reference to ‘fourth parties’ is also intended to capture sub-contracting arrangements, which raises some challenging questions about how far along the supply chain APRA-regulated entities need to go in order to meet their diligence obligations (and what level of diligence will be required).

- A number of significant changes and uplifts have been made around business continuity compared to the current requirements in CPS 232.

- In terms of notifications, a new requirement has been added to report operational risk incidents to APRA. These are not supposed to overlap with CPS 234 notifications, but could do so. In any event, the time period is the same and an incident reported under CPS 234 will not need to be separately reported under CPS 230 (although there may still be overlaps with requirements to report to other regulators such as ASIC, OAIC, ASX, AFP, and ACSC).

- Entities will need to enhance existing processes and establish new processes to comply with CPS 230 and will need to also consider whether uplifts may be required to both existing and new material service provider contracts to facilitate compliance with CPS 230 when it comes into force. The draft CPS 230 does not include a transitionary grace period, but APRA is inviting feedback on what form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers.

KEY DIFFERENCES FROM CURRENT STANDARDS

Below is a snapshot of some of the key differences that are proposed in draft CPS 230 from the current prudential standards on outsourcing and business continuity. Note that this is not a summary of the requirements of CPS 230 or an exhaustive list of differences with CPS/SPS 231 and 232.

ACCOUNTABILITY & GOVERNANCE

- APRA has traditionally referred to the Board as being ‘responsible’ for risk management. Under draft CPS 230, APRA has moved away from passively referring to the Board as ‘responsible’ for risk management and instead uses more active language in describing the Board as being ‘accountable’ for the oversight of an entity’s operational risk management.

- There is also increased accountability on, and reporting to, senior managers (including regular reporting on testing and effectiveness of operational risk controls, performance against service levels by material service providers and compliance by both parties with service provider arrangements) and reporting to the Board (e.g. reporting any failure to meet tolerance levels).

ADDITIONAL POWERS FOR APRA

A number of additional powers for APRA are proposed, including that APRA could:

- require the entity to hold additional capital, impose conditions on the entity’s licence, independent review and remediation if it considers that an entity’s operational risk management has material weaknesses;

- direct that certain business operations are classified as ‘critical operations’ or that a certain service provider or type of service provider is a ‘material service provider’;

- require an entity to review and change its tolerance levels for a critical operation and/or set tolerance levels for an entity or class of entities where it identifies a heightened risk or material weakness; and

- require an entity to review or make changes to a service provider arrangement where it identifies heightened prudential concerns (this does not refer to ‘material’ but presumably it should).

EXPANDED OPERATIONAL RISK REQUIREMENTS

The expanded obligations in relation to operational risk management include:

- more prescriptive requirements in relation to designing, implementing, monitoring and testing operational risk controls in line with the entity's risk appetite and (using similar concepts to CPS 234) 'commensurate with the materiality of the risks being controlled';
- assessment of the impact of the APRA-regulated entity's business and strategic decisions on its operational risk profile and operational resilience as part of its business and strategic planning processes (including assessing impacts of new products, services, geographies and technologies);
- maintaining a comprehensive assessment of the APRA-regulated entity's operational risk profile (including having effective information systems to monitor operational risk and compile/analyse operational risk data, and undertaking scenario analyses);
- a comprehensive risk assessment must be conducted before providing any material service to another party (which on the face of it extends to related parties as well). APRA could require an entity to review/strengthen internal controls if it considers there are heightened prudential risks in such scenarios;
- operational risk incidents and near misses (undefined) must be identified, escalated, recorded and addressed in a timely manner.

MATERIAL SERVICE PROVIDERS

CPS 230 will replace CPS 231 but has broadened the focus from outsourcing of a material business activity to a concept of 'material service providers' and downstream sub-contractors. **Material Service Providers** are those providers (including related parties or connected entities) on which the entity relies to undertake a critical operation or that expose it to material operational risk (including a non-exhaustive list of examples in item 49 and providers that manage information assets classified as critical or sensitive under CPS 234). Examples of new requirements include:

- An entity ‘must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks’. It may be difficult for APRA-regulated entities to judge exactly what this requires. Consideration will also need to be made as to the governance processes needed to support such decisions and what delegations will be put in place to enable the business to continue to operate effectively and efficiently, whilst also complying with these enhanced obligations.

- An entity must maintain a register of Material Service Providers and provide it to APRA annually.

- New requirements around assessing and managing risks, including risks associated with geographic location or concentration of the service provider or parties the service provider relies upon in providing the service.

- The list of matters that contracts for Material Service Provider arrangements must address is shorter than the ‘shopping list’ in CPS 231, but may require some contractual uplift in existing contracts given the expanded scope of Material Service Provider versus outsourcing, the requirement for notification by the service provider of its use of other material service providers and the ambiguity of what provisions may be required to ‘ensure the ability of the entity to meet its legal and compliance obligations’ (see item 53(c)) or ‘ensure the service provider agrees to not impede APRA in fulfilling its duties as prudential regulator’ (see item 54(c)). Helpfully though, the often-debated requirement for an indemnity regarding subcontractors which is present in CPS 231 has not been included (instead CPS 230 simply requires that liability for any failure on the part of a subcontractor be the responsibility of the service provider).

BUSINESS CONTINUITY

A number of changes and uplifts have been made around business continuity compared to the current requirements in CPS 232. These include:

- new concept of tolerance levels;

- new concept of ‘critical operations’, which is defined in a way that is similar but a bit more specific than ‘critical business operations’ in CPS 232 and seems to be somewhat

aligned to the UK, US and EU frameworks. An entity must define, identify and maintain a register of its critical operations;

- an entity must maintain a credible business continuity plan (**BCP**) that sets out how it would maintain critical operations within tolerance levels through disruptions, including disaster recovery planning for 'critical' information assets;

- the Board must approve BCPs and tolerance levels for disruptions to critical operations, review testing results and execution of any findings;

- in relation to internal audit reviews of the BCP, CPS 230 requires assurances to be provided to the Board but does not allow this to be delegated to other management (as currently allowed in CPS 232).

The minimum requirements for BCPs are broadly similar to CPS 232. Interestingly, CPS 230 does not include specific reference to a regulated entity needing to ensure that service providers have BCPs in place (although it is implicitly captured through the concept of critical operations needing to be covered by the BCPs).

NOTIFICATIONS TO APRA

- **Operational risk incidents**: New requirement to notify APRA within 72 hours after becoming aware of an operational risk incident that it determines is likely to have a material financial impact or material impact on the ability of the entity to maintain its critical operations. There could be some overlap with CPS 234 notifications here, but the time period is the same and an incident reported under CPS 234 will not need to be separately reported under CPS 230.

- **Material agreements and offshoring**: Similar requirement to notify within 20 business days of entering into arrangement for a service on which an entity relies to undertake a critical operation or prior to any offshoring with a material service provider, but expanded to also require notification when such arrangements are materially modified.

- **Business continuity**: Similar requirement to notify APRA within 24 hours if the entity has activated its BCP. The timeframe and information required in the notification is the same as CPS 232, but it is interesting that the trigger has been changed from when the entity 'experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness' under CPS 232 to simply activation of the BCP under CPS 230.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PETER JONES
PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com

KATHERINE GREGOR
PARTNER, MELBOURNE
+61 3 9288 1663
Katherine.Gregor@hsf.com

CHARLOTTE HENRY
PARTNER, SYDNEY

+61 2 9225 5733
charlotte.henry@hsf.com

TONY COBURN
CONSULTANT, SYDNEY
+61 2 9322 4976
Tony.Coburn@hsf.com

ANDREW BRADLEY
PARTNER, SYDNEY

+61 2 9322 4455
andrew.bradley@hsf.com

MAGED GIRGIS
PARTNER, SYDNEY

+61 2 9322 4456
maged.girgis@hsf.com

MICHAEL VRISAKIS
PARTNER, SYDNEY

+61 2 9322 4411
Michael.Vrisakis@hsf.com

LEGAL NOTICE