RESPONSE PAPER

Operational Risk Management

17 July 2023

Disclaimer Text

Contents

Executive summary

In July 2022, APRA released for consultation *Discussion paper – Strengthening operational risk management* (Discussion paper) and draft *Prudential Standard CPS 230 Operational Risk Management* (CPS 230).

The management of operational risk is of critical importance, as demonstrated by operational risk failures and business disruptions in the past. All APRA-regulated entities need to ensure that they are well placed to manage operational risk and respond to business disruptions when they inevitably occur.

The aim of CPS 230 is to:

- strengthen operational risk management through new requirements to address identified weaknesses in existing practices;
- improve business continuity planning to ensure that regulated entities are ready to respond to severe business disruptions; and
- enhance third-party risk management by extending requirements to all material service providers that regulated entities rely upon for critical operations or that expose them to material operational risk.

Consultation feedback

Overall, 62 submissions were received in response to the consultation. Submissions were generally supportive of the approach set out in draft CPS 230 and its intended focus, including the incorporation of requirements into a single prudential standard. However, some submissions highlighted areas where it was considered that greater clarity and guidance was necessary or where the draft requirements could have unintended consequences and present practical difficulties in implementation.

This Response paper summarises feedback from industry and other stakeholders to the consultation on draft CPS 230. It also sets out APRA's responses to feedback and the timeline for implementation. In conjunction with this Response paper, APRA is releasing the final CPS 230 and draft guidance for consultation, *Prudential Practice Guide CPG 230 Operational Risk Management* (CPG 230).

Key changes

The key changes to the final standard CPS 230 include:

- easing transition: deferring commencement of CPS 230 to 1 July 2025 and inclusion of transition arrangements for existing service provider arrangements;
- flexibility on prescribed critical operations and service providers: refining the requirement to classify specific business operations as 'critical' and certain service providers as 'material', with an 'unless otherwise justified' provision; and

- modifications so that only *material* arrangements with material service providers are captured in relation to certain requirements, rather than all arrangements.

In addition, APRA has developed comprehensive draft guidance (as set out in CPG 230) to assist regulated entities with the implementation of CPS 230, and address issues raised in submissions.

Next steps

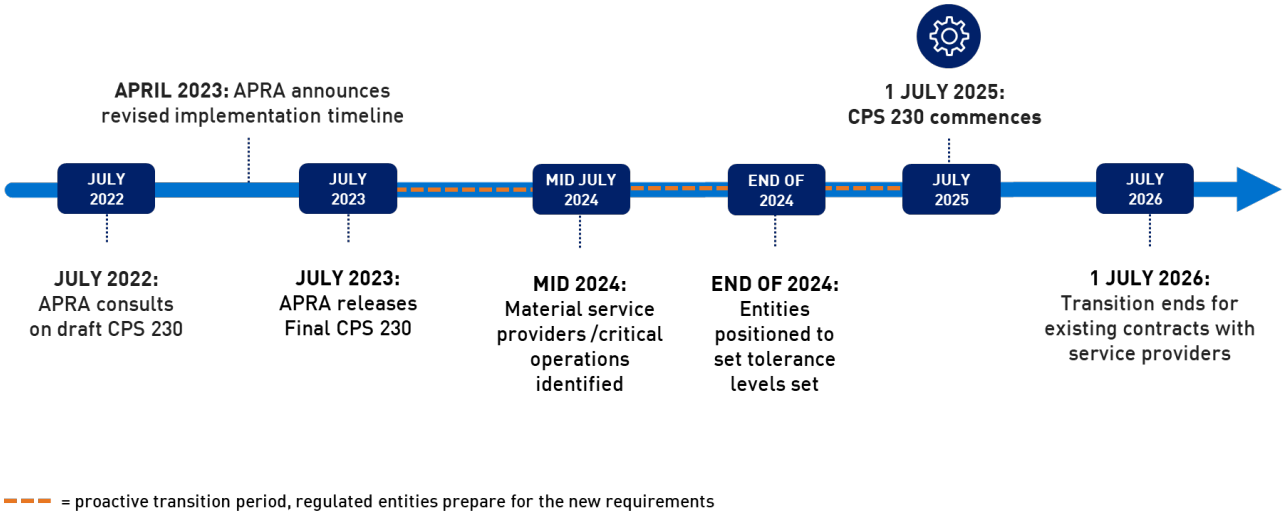
APRA has released the final version of CPS 230 with this Response paper. CPS 230 will commence on 1 July 2025. APRA has included a transition period to allow entities time to update existing contractual arrangements with service providers to comply with CPS 230.

Submissions on CPG 230 are due by 13 October. Following this, APRA expects to finalise the guidance later this year.

While the commencement date for CPS 230 has been moved to 2025, APRA expects regulated entities to be proactive in preparing for the new requirements in 2023-2024: this would include demonstrating meaningful steps and staged progress in moving towards complying with CPS 230, rather than waiting until 2025 to start planning.

The details of staged progress may vary across entities. However, APRA expects there will be some common approaches. For example, APRA expects that senior management would have identified their critical operations and material service providers by mid-2024 and be well positioned to set tolerance levels by the end of 2024. Supervisors will engage with entities during the implementation period to assess progress.

Figure 1.



Glossary

ADI	Authorised deposit-taking institution, as defined in the *Banking Act 1959*
APRA	Australian Prudential Regulation Authority
BCP	Business continuity plan
CPG 230	*Prudential Practice Guide CPG 230 Operational Risk Management*
CPS 230	*Prudential Standard CPS 230 Operational Risk Management*
CPS 234	*Prudential Standard CPS 234 Information Security*
Discussion paper	*Discussion paper – Strengthening operational risk management*, APRA, July 2022
Non-SFI	An entity that is not a significant financial institution
SFI	Significant financial institution

Chapter 1 - Response to submissions

This chapter sets out APRA's responses to key issues raised in consultation on the draft standard, and an outline of changes made as a result in finalising *Prudential Standard CPS 230 Operational Risk Management* (CPS 230).

1.1 Commencement date

APRA originally proposed that CPS 230 would commence on 1 January 2024. This commencement date reflected a balance of considerations: while the proposed CPS 230 is a new standard, existing risk management, business continuity and outsourcing processes should already provide a solid foundation for entities to comply with CPS 230.

Comments received

In general, there was a view from entities that the proposed commencement date would be difficult to meet. Submissions highlighted a number of practical difficulties with the proposed commencement date, including:

- significant planning and resources would be required to implement CPS 230;
- the scope of increases relative to existing requirements;
- the need for guidance to assist entities to implement and comply with CPS 230; and
- various other concurrent regulatory changes, which are already stretching resources.

APRA's response

APRA acknowledges the issues raised on the proposed commencement date of 1 January 2024. APRA will therefore postpone commencement of CPS 230 until 1 July 2025 to provide regulated entities additional time to take the necessary steps to comply with CPS 230.

1.2 Transition

APRA requested feedback on a number of matters to assist in finalising CPS 230. One of these matters was the form of transition arrangements, and the timeframe that would be needed to renegotiate contracts with existing service providers (if required).

Comments received

Submissions commenting on transition were clear in their view that an appropriate transition period was necessary to provide time for entities to ensure existing contractual arrangements would comply with CPS 230.

It was noted that reviewing existing contracts and engaging with service providers will take time. Suggested transition timeframes varied, and typically reflected the size of a regulated

entity and the extent of reliance on third parties for the provision of services. The suggested transition timeframes ranged from one year to three years after commencement of CPS 230, while others suggested contracts should not have to comply until they were next due for renewal, whenever that might be.

APRA's response

APRA acknowledges that entities with existing contractual arrangements will need a reasonable time to review arrangements and take necessary steps to achieve compliance with CPS 230.

APRA has included a transition period in CPS 230 to allow regulated entities time to make changes to existing contractual arrangements with service providers: APRA-regulated entities will have until the earlier of 1 July 2026 or the next renewal date of an existing agreement to ensure the agreement complies with CPS 230. That said, contracts with material service providers should be updated as soon as possible given their importance to critical operations and operational risk.

1.3 Proportionality

APRA sought the views of stakeholders on the question of if, and how, proportionality should be applied to CPS 230. The Discussion paper accompanying the consultation provided examples of possible approaches. One approach would be to apply higher requirements to significant financial institutions (SFIs) relative to non-SFIs. The second approach would be to apply all requirements to all regulated entities, with entities to use their discretion to comply with CPS 230 in a proportionate manner, commensurate with the scale and complexity of their operations.

Comments received

Around one third of submissions commented on proportionality. While there was support for each approach, the overall view tended to be that operational risk management is critical to the successful running of all APRA-regulated entities. As such, distinguishing between SFIs and non-SFIs was not appropriate, and requirements in the standard should apply to all APRA-regulated entities. However, some submissions considered that, as set out in the objectives box in CPS 230, proportionality would best be achieved through an explicit distinction based on the size, complexity and business mix of an APRA-regulated entity (such as SFI/non-SFI).

APRA's response

In consulting on CPS 230, APRA sought input from industry on how best to apply CPS 230 in a way that would achieve the objectives of the standard, while recognising differences in size, business mix and complexity.

After consideration of industry views on this matter, APRA's view is that CPS 230 should apply to all regulated entities. CPS 230 will apply commensurate with the scale, complexity and business mix of an entity's operations. Where relevant, CPG 230 also provides examples of APRA's expectations of how different types of entities would be expected to demonstrate compliance with CPS 230.

1.4 Notification requirements

Draft CPS 230 proposed that a regulated entity must notify APRA:

- of incidents: as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations;
- of BCP activation: as soon as possible, and not later than 24 hours, if it has activated its BCP. The notification would cover the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations;
- of changes to service provider agreements: as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and
- prior to entering into any offshoring agreement with a material service provider, or when there is a significant change proposed to the agreement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.

APRA also sought specific comment as to whether the proposed notification requirements and associated time periods were considered reasonable.

Comments received

The proposed notification requirements generated a significant number of comments. Comments included:

- requests for clarity on how notifications are to be provided to APRA, and the information to be provided;
- requests for reconsideration of the notification timeframes, which some respondents considered would be difficult to meet;
- requests that where an incident or event is captured by notification requirements under more than one prudential standard, an entity only be required to make a single notification to APRA, rather than separately reporting for each relevant notification requirement; and
- that the business continuity planning (BCP) notification is broad and would capture insignificant BCP activations, so requires a materiality threshold or to be qualified in some way.

APRA's response

APRA has provided clarity on notification processes, but has not extended the timeframes. Notifications are a vital mechanism to ensure necessary information is communicated to APRA expeditiously. The notification requirements are not intended to divert an entity from managing an incident or to impose undue burden. As well as ensuring that APRA is kept appropriately informed, notifications allow APRA to respond or assist as necessary, including

considering any potential system-wide implications. While APRA has not extended notification timeframes, updates have been made to simplify the process. This includes:

- a regulated entity only needs to notify APRA if the activation of the entity's BCP relates to a disruption to a critical operation outside tolerance. CPS 230 has been updated to reflect this, with further guidance included in draft CPG 230 released with this Response paper;
- CPS 230 includes a footnote to confirm that a notification of an information security incident under CPS 234 does not need to be separately reported under CPS 230; and
-
- draft CPG 230, released for consultation with this Response paper, provides guidance on APRA's expectations when making required notifications under CPS 230.

1.5 Board requirements

Draft CPS 230 included proposed requirements related to the role of the Board in the oversight of operational risk management, business continuity and service provider management. The proposed requirements reflect that the Board is ultimately accountable for operational risk management. The Board must be provided with appropriate and sufficient information to allow it to effectively discharge its responsibilities and make informed decisions.

Comments received

The section on Role of the Board in draft CPS 230 generated a broad range of comments. A common theme was the risk that APRA's proposals could blur the line between the Board and management by requiring the Board to undertake tasks that would normally be management functions. Examples included:

- setting tolerance levels, which could be granular in some cases;
- approving the service provider management policy – the Board should approve initial policy, but not subsequent updates unless they are material; and
- reviewing risk and performance reporting.

APRA's response

APRA notes that the intent of CPS 230 is not to impose management functions on the Board. Rather, as noted in the Discussion paper, the standard reflects that the Board is ultimately accountable for the oversight of operational risk management and is expected to ensure that senior management effectively implement and maintain a regulated entity's operational risk framework. This reflects a key lesson from the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* on the importance of strong oversight of non-financial risks, with the Board having relevant information to allow it to discharge its responsibilities and make informed decisions.

The intent is not for the Board to play a role in day-to-day operational risk management. Draft CPG 230 provides guidance to assist with interpretation of the requirements imposed on the Board. This includes clarification that while the Board sets overall tolerance levels for disruptions to critical operations, senior management is able to set more granular tolerance levels for critical operations within the Board-approved tolerance levels.

1.6 Definition of operational risk

Draft CPS 230 included a requirement that an APRA-regulated entity must identify, assess and manage operational risks that 'may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events.'

Comments received

A number of submissions commented that the definition of operational risk in draft CPS 230 differed from existing definitions in other APRA prudential standards. Submissions highlighted issues with using different definitions and sought clarity from APRA on this.

In addition, there were comments on the reference in draft CPS 230 to specific types of operational risk including legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management. Submissions queried the inclusion of some of these risks as part of operational risk; notably, reputational risk, which many considered to be an impact or outcome of an operational risk incident, rather than an operational risk itself.

APRA's response

APRA will review existing definitions of operational risk in the prudential framework for consistency with the definition of operational risk in CPS 230.

APRA has removed reputational risk from the list of risks included as part of operational risk, but otherwise retained the definition and references to specific types of operational risk. APRA considers these risks have a clear connection to operational risk and should be considered and dealt with as part of a regulated entity's operational risk management.

The removal of reputational risk reflects that typically reputational risk is treated as an outcome of an operational risk incident or event rather than an operational risk itself. However, a regulated entity would still be expected to give consideration to the reputational impact of an operational risk event on the entity.

1.7 Critical operations

Draft CPS 230 set out a number of key requirements intended to ensure that an APRA-regulated entity's business continuity planning would:

- to the extent practicable, prevent disruptions to its critical operations; and
- include measures to adapt systems and processes so that the entity can continue to operate in the event of a disruption and return to business-as-usual operations promptly thereafter.

Draft CPS 230 defined critical operations as processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers or the entity's role in the financial system. In addition, draft CPS 230 included a proposed list of operations that would be classified as critical.

Comments received

The business continuity section of draft CPS 230 was commented on by a number of submissions. While most sought clarification of certain provisions and specific guidance on APRA's expectations to assist in implementation, some concerns were expressed on the proposed list of prescribed critical operations.

The issues raised were that:

- the inclusion of a prescribed list of specific business operations that should be classified as critical undermines the general principles-based definition of critical operations;
- the breadth of the list is such that it may capture non-critical operations for some entities;
- not all critical operations specified are relevant to all APRA-regulated industries and, if retained, the list should be classified by industry to assist with clarity;
- the specific inclusions appear to be focused more on internal processes, rather than the outcome of those operations; and
- each of the prescribed critical operations is very broad and does not allow for consideration of the details or context of the operation in question.

APRA's response

As noted in the Discussion paper, the intent of prescribing critical operations was to ensure consistency of application across APRA-regulated entities. Noting the concerns that have been raised, APRA has qualified the list of prescribed critical operations in CPS 230: a regulated entity may classify a prescribed operation as not critical if it can provide satisfactory justification for its decision. APRA expects that these cases will be exceptional.

Draft CPG 230 provides further guidance, with better practice being a rigorous assessment of the business operation in question. The review and decision should be documented, approved by an accountable person[1] or other appropriate senior management, and reviewed at least

[1] An accountable person means a person who is an accountable person under the Financial Accountability Regime.

annually. APRA may still require a regulated entity to classify the operation as a critical operation if APRA disagrees with the entity's assessment.

1.8 Material service providers

Draft CPS 230 prescribed certain services as being material.

Comments received

The proposed inclusion of a prescribed list of material service providers generated a significant proportion of comments in submissions. Submissions were generally against the inclusion of the prescribed list of material service providers. Issues raised included:

- the list is not consistent with the principles-based approach of the standard and the intention that a regulated entity determine which of its service providers are material;
- the prescribed list may lead to outcomes where providers of services that are not material are captured as material service providers; and
- certain proposed prescribed material service providers, in some cases, do not provide the service to the regulated entity but rather to their customers. Examples cited included insurance brokers and mortgage brokers.

APRA's response

Noting the concerns that have been raised, APRA has qualified the list of prescribed material service providers in CPS 230: a regulated entity is still required to classify prescribed service providers as material service providers but may decide not to do so provided the regulated entity can justify its decision. APRA expects that these cases will be exceptional.

Draft CPG 230 provides guidance that a regulated entity may decide not to classify a service provider as material where it has undertaken an assessment of the service provider in question and has appropriate oversight of the decision. APRA may require the regulated entity to classify the service provider as material if APRA disagrees with the regulated entity's assessment.

APRA has also sought to provide further clarity in CPS 230 to the effect that it is only material arrangements with material service providers that are captured by certain requirements in the prudential standard. Relevant provisions of CPS 230 have been amended to reflect this. Not all arrangements with a material service provider will be material to the entity. 'Material arrangements' are those on which a regulated entity relies to undertake a critical operation or that expose the entity to material operational risk.

1.9 Register of material service providers

Draft CPS 230 proposed that an APRA-regulated entity include the register of the entity's material service providers as part of its service provider management policy.

Comments received

While there was general support for the maintenance of a register of material service providers, submissions did not support the register forming part of a regulated entity's service provider management policy. Various concerns were expressed, most notably that the policy would need to be updated whenever there were changes to the register of material service providers, which could be onerous for many entities for what should be a simple administrative update.

APRA's response

APRA notes the potential administrative burden caused by including the register of material service providers as part of the service provider policy. The final CPS 230, while still requiring the maintenance of a register of material service providers, does not require this to form part of a regulated entity's service provider management policy.

1.10 Providers that manage information assets

Draft CPS 230 proposed that all service providers that manage information assets classified as critical or sensitive under CPS 234 would be classified as material service providers.

Comments received

A number of submissions expressed concern about this requirement. Specifically, there were concerns that the number of material service providers would increase significantly and may inadvertently capture providers that are not material.

APRA's response

Noting the practical issues and concerns raised by entities, APRA has removed this requirement from the final CPS 230. Such providers would, however, still be captured where they meet the broad definition of material service provider set out in the final CPS 230.

1.11 Cloud information paper

In September 2018, APRA updated its information paper on cloud computing, *Outsourcing involving cloud computing services*.

Comments received

A number of submissions sought clarification on the status of the Cloud information paper in light of APRA's proposals on operational resilience and CPS 230.

APRA's response

APRA's Cloud information paper remains current. APRA will, at an appropriate future time, undertake a full review of the Cloud information paper. In the interim, regulated entities should continue to have regard to the practices and key principles outlined in the Cloud information paper when entering into or making changes to cloud computing arrangements and continue to engage with APRA on the use of Cloud.

Chapter 2 - Consultation on Prudential Practice Guide CPG 230

In conjunction with this Response paper, APRA has released draft CPG 230 for consultation. Draft CPG 230 provides guidance to assist with the implementation of CPS 230 and includes specific content to address various issues raised in submissions on draft CPS 230.

Draft CPG 230 has been prepared based on the final version of CPS 230 released with this Response paper and is provided in an integrated format that maps the guidance to the relevant paragraphs in CPS 230.

2.1 Key elements of CPG 230

Draft CPG 230 aims to assist APRA-regulated entities in both implementing and meeting the requirements of CPS 230 on operational risk management, business continuity and service provider management. It also incorporates guidance to address key issues and concerns raised by submissions in response to the CPS 230 consultation. Key areas of guidance are highlighted below.

Role of the Board

Draft CPG 230 provides guidance on APRA's expectations of the Board and senior management in fulfilling their respective responsibilities under CPS 230. Draft CPG 230 also provides further guidance on APRA's expectations of the Board in its oversight of operational risk, business continuity and material service provider arrangements.

Operational risk management

Draft CPG 230 provides specific guidance on the extent of monitoring of operational risk management generally, as well as more detailed guidance on the assessment of the entity's operational risk profile, including for new products; identifying and documenting end-to-end processes; and scenario analysis and control design, monitoring and testing.

Business continuity

Draft CPG 230 provides guidance on identifying critical operations, setting associated tolerance levels and business continuity planning, including APRA's expectations around systematic testing.

Service provider management

Draft CPG 230 provides guidance on typical areas that would be addressed by an entity's service provider management policy, managing risks at all stages of the arrangement and managing risks associated with fourth parties and other downstream providers.

Notifications

CPS 230 requires notification of certain matters to APRA. Draft CPG 230 provides guidance on the type of information a regulated entity would typically be expected to provide and how the information can be provided to APRA.

2.2 Request for submissions

APRA invites written submissions on draft CPG 230. Submissions should be sent to PolicyDevelopment@apra.gov.au by 13 October 2023 addressed to the General Manager, Policy, APRA.

Following review of feedback received through submissions, APRA aims to finalise CPG 230 later this year for industry to utilise CPG 230 in preparing for the commencement of CPS 230.

Important disclosure notice — publication of submissions

All information in submissions will be made available to the public on the APRA website unless a respondent expressly requests that all or part of the submission is to remain in confidence. Automatically generated confidentiality statements in emails do not suffice for this purpose. Respondents who would like part of their submission to remain in confidence should provide this information marked as confidential in a separate attachment.

Submissions may be the subject of a request for access made under *the Freedom of Information Act 1982* (FOIA). APRA will determine such requests, if any, in accordance with the provisions of the FOIA. Information in the submission about any APRA-regulated entity that is not in the public domain and that is identified as confidential will be protected by section 56 of the *Australian Prudential Regulation Authority Act 1998* and will therefore be exempt from production under the FOIA.

APRA