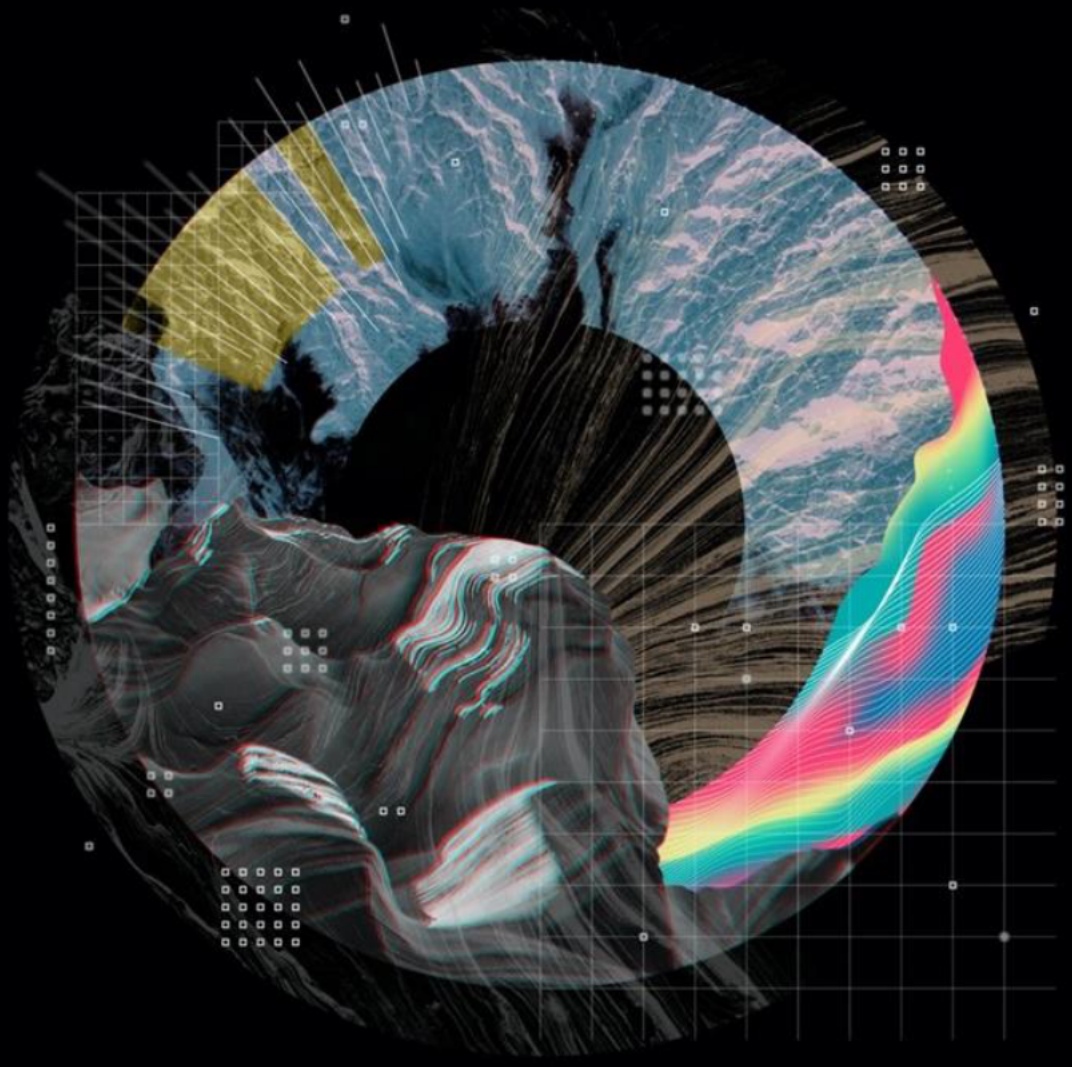

Draft Prudential Practice Guide CPG 230

Operational Risk Management

Deloitte response to consultation

13 October 2023

Deloitte.

Deloitte Touche Tohmatsu
Quay Quarter Tower
50 Bridge Street
Sydney NSW 2000
Australia
Tel: +61 2 9322 7000
www.deloitte.com.au

General Manager, Policy
Australian Prudential Regulation Authority
By email: PolicyDevelopment@apra.gov.au

Dear [redacted]

Deloitte response to consultation on the draft Prudential Practice Guide, CPG 230 *Operational Risk Management*.

Please find enclosed the Deloitte submission in response to consultation on the draft Prudential Practice Guide, CPG 230 Operational Risk Management (CPG 230).

Deloitte supports APRA's objectives and principles-based approach outlined within the final Prudential Standard and draft Prudential Practice Guide. In finalising CPG 230, Deloitte welcomes the opportunity to provide feedback and have identified key principles and considerations based on our on global and local experience in Operational Resilience.

We welcome the opportunity to discuss this topic in more detail if required.

Yours sincerely,

[redacted]
Partner, Risk Advisory
Operational Resilience Lead Partner, Australia
Deloitte Touche Tohmatsu

[redacted]
Partner, Risk Advisory
Financial Industry Risk & Regulation
Deloitte Touche Tohmatsu

Response to Consultation

This section outlines our responses to the proposed CPG 230. These are based on our local and global experience in operational resilience, as well as our extensive experience working with financial services institutions to plan, design and implement regulatory change programs.

1.1 General

Deloitte Australia is supportive of APRA's proposed CPG 230.

The draft Prudential Practice Guide provides helpful clarification of the intent of *CPS 230 Operational Risk Management* (CPS 230 or the Standard) and APRA's expectations of regulated entities ("entities") planning for and implementing the new Standard. The inclusion of better practice principles will also support more consistent application of the Standard, and help drive operational resilience across the financial services industry.

However, further guidance on the following areas would assist entities in successfully navigating their implementation programs.

1.1.1 Compliance and assurance by 1 July 2025

Additional guidance on APRA's expectations in relation to compliance by 1 July 2025 would be beneficial. It is expected that many entities will need to undergo remediation to bring Critical Operations within tolerance, and to address any operating effectiveness weaknesses in operational risk, business continuity or Service Provider management practices identified as implementation progresses. This is in addition to efforts required to bring the design of frameworks, policies, processes, technology, and capability in line with the Standard. Clearer guidance on the expected status of these remediation activities by the effective date will allow entities to better prioritise their finite resources. In our view this remediation effort (if required) should be treated as additional effort, and having a robust plan with clear deliverables and appropriate timeframes for remediation would be sufficient as at 1 July 2025.

Given the expected scale and complexity of change that entities will undergo to comply with CPS 230, further guidance on the degree of assurance expected from APRA would also be helpful. This would encompass assurance over the governance of the implementation program, as well as the interpretation of the Standard and appropriateness of uplift activities.

1.1.2 Data requirements and linkage to APRA's five-year roadmap

As APRA indicates in the guidance, data quality will be an important enabler of compliance with CPS 230. For many entities, this will be an area requiring uplift. APRA's five-year roadmap for data collections, including non-financial risk collections in 2024, will likely drive remediation activity in the data space. It would therefore be helpful for APRA to provide further guidance on specific considerations and expectations that will enable entities to maximise data remediation efforts across CPS 230 compliance and preparation for non-financial risk collections.

1.2 Operational Risk Management

1.2.1 Operational risk classes

The Standard provides guidance on expected risk classes which fall under the definition of operational risk. A more exhaustive list to ensure alignment with APRA's expectations would be helpful. For example, many organisations today have defined Cyber risk as a separate category outside of operational risk.

1.2.2 Risk profiling by Critical Operations

A reasonable implication of CPS 230 is that entities will need to develop a view of their operational risk profile by Critical Operation. To build this view, entities will likely need to piece together disparate data sets across different systems and from outside entity boundaries (for Service Provider-related risk data). This profile would need to be

detailed enough to provide an accurate view of operational risk weaknesses specific to the Critical Operation, yet not too detailed so as to inhibit meaningful insight and decision making by the Board and senior management. Further guidance or illustrative examples from APRA would help organisations navigate this challenge.

1.3 Business Continuity Management

1.3.1 Alignment and distinction between Critical Operations (CPS 230) and Critical Functions (CPS 900)

We believe further guidance and updated examples on how the concepts of Critical Operations (CPS 230) and Critical Functions (CPS 900) align and differ would be beneficial. In the definitions provided, APRA refers to Critical Operations as '*a process*' and Critical Functions as '*a function*'. It remains uncertain whether the terms '*process*' and '*function*' are considered synonymous.

Definitions will impact the approach taken to articulate Critical Operations and Critical Functions (i.e., how these are worded and the level of granularity at which they are described), how they fit in an entity's wider process architecture, and the extent to which risk management arrangements can be leveraged, re-purposed or standardised.

APRA has provided the following examples:

- Critical Operations – payments, deposit taking and management (CPS 230)
- Critical Functions – very large deposit book (discussion paper '*Strengthening Operational Risk Management*').

It is ambiguous whether in APRA's view a '*process*' differs from a '*function*', and whether APRA expects Critical Operations and Critical Functions to be described differently.

Conversely, draft CPG 230 suggests that references to '*process*' and '*function*' are synonymous, and Critical Functions and Critical Operations should be articulated in a consistent manner given "*APRA expects that 'critical functions' defined for resolution planning would be classified as critical operations" (*draft CPG 230*,* paragraph 61*)*.

Acknowledging that APRA's view of Critical Functions may have evolved, we are of the view that entities would benefit from updated examples to better illustrate how Critical Functions should differ or align with the Critical Operations examples given by APRA. Guidance on how entities can comply with both standards in a more integrated manner would also be welcomed.

If, however, the Critical Functions example of '*very large deposit book*' still reflects APRA's expectation, and APRA also expects Critical Functions to be classified as Critical Operations, there may be potential:

- Misalignment between how these are described within an entity, resulting in a need to 'map' linkages between Critical Functions and Critical Operations to ensure coverage.
- Duplicative efforts and siloed approaches to CPS 230 and CPS 900 implementation, resulting in significant ongoing compliance costs.

To illustrate these concepts, and the intersections between CPS 230 and CPS 900, APRA may consider offering guidance akin to the guidance provided by the UK Prudential Regulatory Authority (PRA) on this topic (noting there may be variations across regulatory frameworks). In particular, the PRA's Policy Statement 'PS6/21 Operational resilience: Impact tolerances for important business services (March 2021) and sections on '*Important business services, critical functions, and critical services*' and *'Example of the interaction of critical functions, critical services and important business services'.*

1.3.2 Expectations on internally focused processes

In CPS 230 and draft CPG 230, APRA has placed emphasis on Critical Operations being externally focused and expects entities "*in identifying its critical operations […] would focus on outward-facing services that it needs to continue to run to support external stakeholders*" (draft CPG 230, paragraph 59).

There are a number of internally focused processes that will not meet APRA's definition of a Critical Operation but are still important for the day-to-day running of an entity (e.g., payroll). These internal-facing processes deliver an

internal outcome but may have an indirect material adverse impact on external stakeholders if disrupted given their impact on internal stakeholders.

Previously, these would have been identified under *CPS/SPS 232 Business Continuity Management*. However, depending on the approach taken for mapping Critical Operations (incl. granularity level), these internal processes may not necessarily be captured going forward, and as a result, may not have the contingency arrangements needed to minimise the impacts of a disruption.

We note that prudent entities will continue to include these in the scope of their business continuity management programs but may not impose the same operational resilience requirements on them as they would for Critical Operations. However, to enable consistency across the industry, more explicit guidance from APRA on this matter will support entities as they review their approach for managing the risks associated with these internal processes.

1.3.3 Tiering of tolerance levels

Draft CPG 230 suggests that Board-approved tolerance levels may be complimented with more granular tolerance levels and indicators. As examples, APRA has stated that entities may wish to reflect tolerance levels for specific types of payments in particular jurisdictions, or specific processes that form part of a Critical Operation.

If implementing the approach suggested by APRA in draft CPG 230, Critical Operations would likely need to be defined at different levels of granularity to enable this:

- Board-approved tolerance levels would need to be set against overarching Critical Operations
- Senior Management-approved tolerance levels would be set against granular Critical Operations (or 'critical processes or activities' to avoid potential confusion over terminology).

In doing so, there is a risk that overarching Critical Operations are being defined too broadly which could result in overly conservative tolerance levels being set and heightened operational resilience standards being imposed on areas that may not necessarily require it.

Additionally, CPS 230 describes tolerance levels as being inclusive of:

a) the maximum period of time the entity would tolerate a disruption to the operation;

b) the maximum extent of data loss the entity would accept as a result of a disruption; and

c) minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

It is unclear whether the Board-approved tolerance level should include individual measures of the maximum data loss tolerable for each key data set that supports the delivery of Critical Operations or whether APRA expects an aggregated measure of the maximum data loss tolerated for all key data sets related to a Critical Operation. The latter would likely result in a low tolerance for data loss on a broad range of data sets, including those that may not necessarily be as critical.

As entities determine the granularity at which they will frame Critical Operations and their approach for setting Tolerance Levels, further guidance from APRA on how entities can set meaningful Board-approved and Senior Management-approved tolerance levels would be helpful.

1.4 Service Provider Management

1.4.1 Structure for material Service Provider register

Entities are required to maintain and submit a register of their material Service Providers on an annual basis (CPS 230, paragraph 51). The draft CPG 230 states that "*better practice is for the register to contain all service providers and services, with material providers clearly identified" (draft CPG 230, paragraph 95).*

Similarly to APRA's guidance with respect to the Critical Operations Register (draft CPG 230, paragraph 54), APRA should consider specifying minimum information to be captured for material Service Providers and provide more

explicit guidance on the structure and format of the register. In addition to promoting consistency across the industry, this will also support APRA in its supervisory activities and enable more effective analysis.

1.4.2 Materiality assessment criteria

Service Providers

Material Service Providers are defined within CPS 230 as those "*on which the entity relies to undertake a critical operation or that expose it to a material operational risk" (CPS 230, paragraph 49).* Given the subjective nature of the term "*relies*", this criterion may raise questions over the volume of material Service Providers that may be captured under the wording of this requirement.

Further guidance on the degree of reliance that may require a Service Provider to be classified as material, including materiality assessment criteria will reduce ambiguity and enable a more accurate classification of Service Providers. Alternatively, if the intent of CPS 230 is for entities to capture *all* Service Providers involved with the delivery of a Critical Operation, regardless of the nature, scale and size of the services provided, APRA should consider making this more explicit in the Prudential Practice Guide.

CPS 230 also includes a revised materiality threshold for Service Provider arrangements, notably with the inclusion of the following wording "*Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk." (CPS 230, paragraph 49)*. The revised threshold reduces the scope of arrangements with material Service Providers to only those that are determined as material, given entities may also have non-material arrangements with material Service Providers. However, as above, the use of the term "relies" presents similar potential challenges that can be addressed through the inclusion of clearer guidance in CPG 230.

Fourth parties

A Service Provider's material risk weaknesses may have an indirect operational impact on the entities they provide services to. For example, if a Service Provider is exposed to a material risk from other Service Providers they rely upon (that is, a fourth party), this may disrupt how effectively they can support the delivery of an entity's Critical Operation or cause an indirect operational risk to the entity. As such, it may be necessary to consider material risks to the Service Provider when entities assess fourth party risk.

The inclusion of further guidance on APRA's position on fourth party risk would be helpful. That is, whether entities should be supplementing their own assessments with materiality concerns for the Service Provider.

Key Authors and Contributors

[redacted]
Partner, Risk Advisory
Operational Resilience Lead Partner, Australia
[redacted]

[redacted]
Partner, Risk Advisory
Financial Industry Risk & Regulation
[redacted]

[redacted]
Director, Risk Advisory
Financial Industry Risk & Regulation
[redacted]

[redacted]
Director, Risk Advisory
Financial Industry Risk & Regulation
[redacted]

[redacted]
Manager, Risk Advisory
Financial Industry Risk & Regulation
[redacted]

Deloitte.