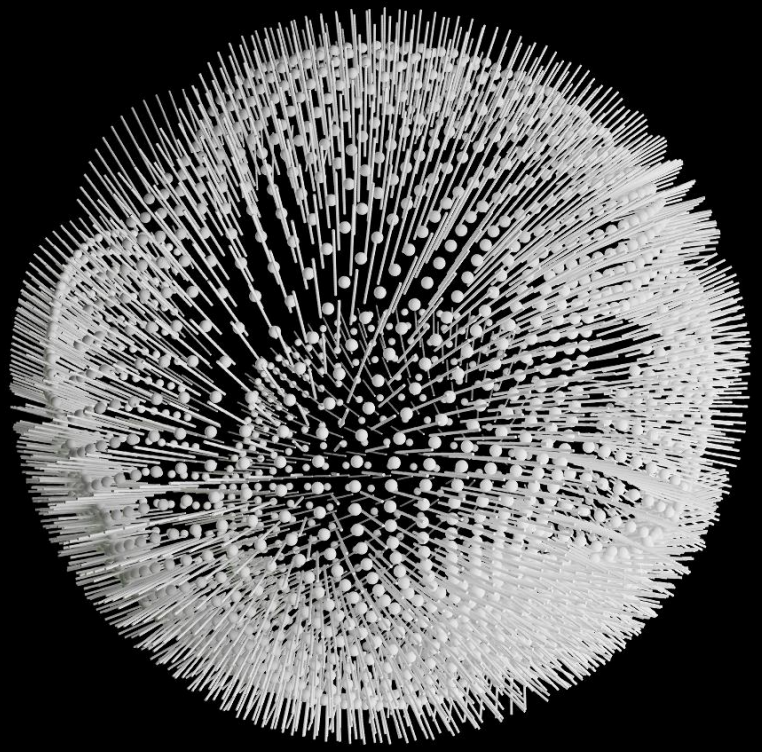
Deloitte.



CPS 230 Operational Risk Management

Initial Perspectives on APRA's draft CPG 230

August 2023

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

Introduction

On 17 July 2023, APRA published the final CPS 230 Operational Risk Management Standard alongside a draft Prudential Practice Guide (CPG 230).

Draft CPG 230 has been designed to support Regulated Entities in their planning and implementation of CPS 230, and sets out APRA's expectations and views on industry better practices.

While the Prudential Guide is under consultation until 13 October 2023 and therefore may be subject to change, regulated entities should proactively reflect on the approach taken to date and assess the potential implications of APRA's draft guidance and what it means for them.

For some entities, aspects of the proposed guidance will validate assumptions made to date. For others, it may give rise to practical challenges or require adjustments to their compliance approach.

The consultation process is an opportune time for entities to consider the impact of the proposed guidance given the context of their organisation and provide feedback before the prudential guide is finalised.

In this release, we focus on certain aspects of APRA's draft CPG 230 and share our initial perspectives, key considerations and where appropriate, illustrative examples on:

1. Granularity of Critical Operations;
2. Board-approved Tolerance Levels and Senior Management-approved Tolerance Levels;
3. Service Provider Risk Management; and
4. Impacts of Board decisions on Operational Resilience.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

1. Granularity of Critical Operations

A question that many entities are asking themselves is "*At what level of detail should Critical Operations be defined?*".

APRA recognises that proportionality is key and the level of detail will vary depending on the size and complexity of the entity.

CPS 230 is intended to be principles-based and as a result, the supporting guidance is not intended to provide a definitive view on granularity. APRA has acknowledged that proportionality is key and the level of detail will vary depending on the size and complexity of the entity.

There may be an inclination to define Critical Operations at a high level for simplicity and clarity. Doing so would result in a shorter and more succinct list of Critical Operations that may make it more manageable for Boards, Senior Management and other key stakeholders to digest and maintain oversight.

However, taking an approach that is too high level may not support accurate identification of process and resource dependencies, risks and vulnerabilities. Further, it may be difficult to set meaningful Tolerance Levels if there is significant variability in disruption impacts for a given Critical Operation.

A more granular description of Critical Operations would also allow for more precise Tolerance Levels to be set. This could prevent situations where overly conservative Tolerance Levels are imposed upon areas that may not necessarily require the same level of resilience.

The onus is on regulated entities to determine the most appropriate approach for their organisation, while ensuring the spirit and intent of CPS 230 is being met. It is worth noting that the approach taken to define Critical Operations will impact subsequent activities such as process and dependency mappings, the setting of Tolerance Levels, as well as ongoing monitoring, testing and assurance activities.

Examples of Critical Operations
For illustrative purposes only

Banking	Superannuation / Wealth	Insurance
• Withdrawing Cash • Making and receiving electronic payments • Accessing account information	• Receiving pension payment • Receiving a TPD insurance claim payment • Accessing account information	• Making an insurance claim • Receiving insurance claim payment • Accessing account information

Note: the above examples are based on our local and global experience in jurisdictions with comparable regulatory frameworks.

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

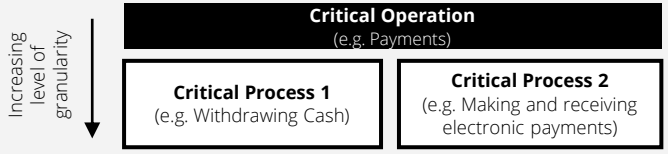
1. Granularity of Critical Operations (continued)

The approach taken to identify Critical Operations will influence the entity's ability to map dependencies, assess the impact of a disruption, and set meaningful Tolerance Levels.

Entities should be mindful of these dependencies when determining their approach.

Example Case Study: Potential implications of broadly defined Critical Operations on Tolerance Levels

For illustrative purposes only



- Entity XYZ has defined '***Payments***' as a Critical Operation to provide coverage for processes related to '***Withdrawing Cash***' and '***Making and receiving Electronic Payments***'.
- Entity XYZ has assessed that it has a lower tolerance for disruption for '***Making and receiving an electronic payment***' compared to '***Withdrawing Cash***' *(i.e.* an inability to make or receive electronic payments during a disruption would cause material adverse impact sooner, compared to an inability to withdraw cash)
- The overarching Board-approved Tolerance Level needs to consider the impacts of the most critical process included in the overarching Critical Operation. As such, the overarching Tolerance Level for '***Payments***' has been set conservatively to reflect the potential impacts of a disruption to '***Making and receiving an electronic payment***'.
- Despite not being as critical, processes related to '***Withdrawing Cash***' are now subject to more stringent Tolerance Levels and will require investment to ensure lower Tolerance Levels can be met.

Note: the above is a fictitious example designed to illustrate potential implications of broadly defining Critical Operations.

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

1. Granularity of Critical Operations (continued)

When determining granularity, entities keep in mind the spirit and intent of the Standard, and ensure the approach taken doesn't limit their ability to meet requirements.

At its core, the Standard seeks to ensure regulated entities:

- understand which aspects of their organisation are most critical;
- have identified where they may be vulnerable and have taken proactive steps to address vulnerabilities; and
- are confident they are sufficiently prepared for disruptions, and that this confidence is backed by proven capabilities.

Taking a considered and justified approach centred on these objectives will help guide entities through implementation activities.

Key considerations

Entities should consider the following when fine-tuning the granularity of Critical Operations:

- Does the articulation **enable a clear and consistent understanding** of what the Critical Operation encompasses?
- Would it enable us to reasonably map process and resource dependencies, and **identify where risks and vulnerabilities exist?**
- Would we be able to **describe the specific impacts of a disruption to the Critical Operation**, and where and when Material Adverse Impact would be caused?
- Would we be able to **set meaningful Tolerance Levels** and other metrics that enable monitoring of Critical Operations and detection of any potential or actual breaches in Tolerance Levels?
- Does it enable us to **direct our focus and investment** on Operations that could cause Material Adverse Impact, and conversely, identify where efforts can be deprioritised or reallocated?

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

2. Board-approved Tolerance Levels and Senior Management-approved Tolerance Levels

The draft CPG 230 suggests that entities may compliment Board-approved Tolerance Levels 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.

As per CPS 230, for each Critical Operation, entities must establish Tolerance Levels for:

(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.

Key considerations

The ability to set *meaningful* Tolerance Levels will depend on Critical Operations being defined with sufficient granularity such that:

- Key dependencies across people, facilities, service providers, technology and information can be clearly identified and mapped (this will help inform (B) above);
- Service levels during normal operations can be easily defined and measured (this will inform (C) above) ;
- The impacts of a disruption can be described and validated (this will inform (A)-(C) above).

To set Board-approved and Senior Management-approved Tolerance Levels, regulated entities would need to define Critical Operations at different levels of granularity.

If implementing the approach suggested in draft CPG 230, Board-approved Tolerance Levels would need to be set against overarching Critical Operations while Senior Management-approved Tolerance Levels would be set against granular Critical Operations (referred as 'Critical Processes' in this paper to avoid potential confusion over terminology).

Entities should ensure overarching Critical Operations are not defined too broadly. As illustrated in the ***Example Case Study*** on page 5, doing so could otherwise result in overly conservative Tolerance Levels being set and approved by the Board, and as such, impose heightened operational resilience standards in areas that may not necessarily require it.

Additionally, regulated entities would also need to ensure triggers for APRA notifications are clearly defined and understood.

Specifically, regulated entities would need to determine and clearly document whether their organisation would notify APRA when a Board-approved Tolerance Level is (or is at risk of being) breached, or whether APRA would also be notified when a Senior Management-approved Tolerance Level is (or is at risk of being) breached. Provided Tolerance Levels set by the Board and Senior Management are aligned and consistent, a breach in one, would also entail a breach of the other.

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

3. Service Provider Risk Management

Where a Service Provider manages controls on behalf of an entity, regulated entities are expected to have visibility of their effectiveness. Service providers should be able to demonstrate *prudent risk management.*

APRA expects entities to take reasonable steps to ensure that their Service Providers' risk management practices do not fall below those that the entity would implement if the service was maintained internally.

In other words, the risks associated with the services and processes performed by Service Providers on behalf of the entity should be managed with the same level of rigour as if those services and processes were performed in-house. APRA has stated that this includes developing process maps for *all* services, including those delivered by Service Providers on behalf of a regulated entity, and validating them through on-site visits and controls monitoring.

An entity's ability to effectively manage the risks associated with Service Provider arrangements is dependent on having open and collaborative relationships. Entities should focus on transparent and frequent communication, clear and measurable performance metrics, and contract clarity.

Key considerations

As entities review their approach to managing Service Providers, they may wish to consider the following:

- **Identify relationship managers** to foster collaboration and open communication with Service Providers, and enable more effective ongoing oversight.
- Where practical, **involve Service Providers when mapping Critical Operations and testing Business Continuity Plans.** This supports greater visibility of key activities performed by the Service Provider, the extent of their reliance on fourth parties, where key handover points and interdependencies exist, and the Service Provider's readiness for disruption.
- **Agree how Service Providers will identify and manage risks, controls, obligations, incidents and issues** to support alignment and consistency in operational risk management practices.
- **Review and challenge whether sufficient and *meaningful* information is being provided by Service Providers** to support the identification of emerging risks and vulnerabilities and informed decision making.
- **Conduct regular reviews, on-site visits and independent assessments of Service Providers.**
- **Review, and where required revise, contractual agreements** to support the above steps and ratify robust risk management practices.

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Perspectives on draft CPG 230

APRA's draft Prudential Practice Guide sets out APRA's perspectives on how best to plan and implement CPS 230, and is currently under consultation.

4. Impacts of Board decisions on Operational Resilience

Entities need to ensure Boards understand the impacts of their strategic decisions on the operational resilience of Critical Operations.

APRA notes that Boards have not consistently been provided with sufficient operational risk information when making strategic decisions.

The final Standard includes a requirement for entities to assess the expected impacts of Board decisions on the operational resilience of Critical Operations.

To effectively support Board decision making, entities will need to:

- Have an end-to-end understanding of their Critical Operations, including process and resource dependencies;
- Identify the types of Board decisions that may impact the operational resilience of Critical Operations;
- Define and agree the attributes of an operationally resilient organisation (e.g. design principles setting out how an operationally resilient organisation is structured and operating). This will help inform how Board decisions might affect (either positively or negatively) the operational resilience of Critical Operations and form the basis of a consistent assessment criteria; and
- Identify data required to support the impact assessment, and ensure that the data is reliable and accurate.

When developing impact assessment criteria for Board decisions, entities should have a clear view of what being operationally resilient means to them.

As an example, entities could define operational resilience by design principles that reflect the attributes of an operationally resilient organisation across People, Facilities, Service Providers and Technology and Data:

- **People** – *There is dual capacity in key responsibilities to mitigate single points of failure.*
- **Facilities** – *Critical Operations are performed across two or more locations that are sufficiently far apart to minimise geographic concentration risk.*
- **Service Providers** – *Single reliance on a sole Service Provider is avoided where feasible, and there are contingency arrangements in place to support the continued provision of services.*
- **Technology and Data** – *Systems which support Critical Operations are configured so that the services have access to mirrored data in each Data Centre in real time.*

Note: Perspectives outlined in this section are based on APRA's draft prudential guide CPG 230 which may be subject to change following industry consultation.

Key Contacts

Caroline Brell
Operational Resilience
Lead Partner
cbrell@deloitte.com.au

Katharine Goulstone
Partner, Financial Industry
Risk and Regulation
kgoulstone@deloitte.com.au

Tarah Unn
Director, Financial Industry
Risk and Regulation
tunn@deloitte.com.au

Kerri Hie
Director, Financial Industry
Risk and Regulation
khie@deloitte.com.au

Suleigh Huang
Manager, Financial Industry
Risk and Regulation
sulhuang@deloitte.com.au

Deloitte.