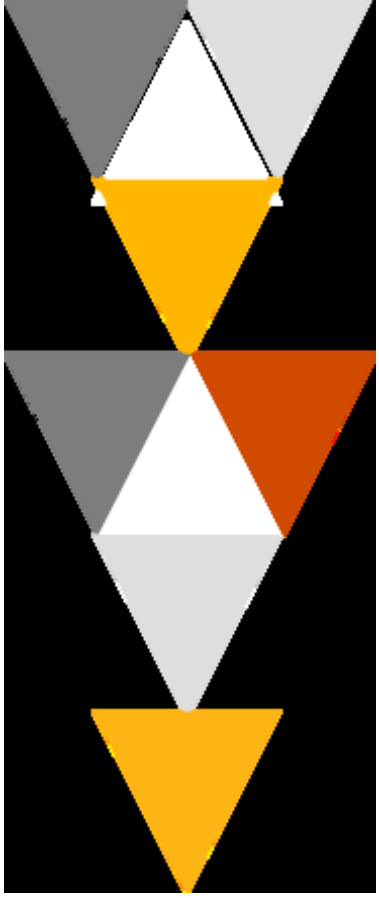

# Prudential Standard CPS 230 Operational Risk Management - Consultation Paper

PwC Submission

October 2022

pwc

pwc

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

via email: PolicyDevelopment@apra.gov.au

21 October 2022

Dear Sir/Madam,

**PwC Submission – Consultation on Draft Prudential Standard CPS 230 – Operational Risk Management**

PwC Australia (PwC) welcomes the opportunity to provide this submission in relation to APRA's draft Prudential Standard CPS 230 – Operational Risk Management (proposed standard).

The proposed standard is important for regulated entities as it will support them with focusing on preventative measures to improve overall operational resilience, through effective operational risk, business continuity and service provider management practices.

With resilient-by-design principles at its core, the proposed standard will complement existing standards such as Prudential Standard CPS 234 – Information Security. Together, they will work to enhance operational resilience, minimising the impact of disruptions to customers and the financial system and increasing the focus of Boards and senior management.

APRA's regulated entities are central to the safe and efficient operation of the Australian economy and the community more broadly, providing access to core financial mechanisms. In a rapidly evolving disruptive environment, the proposed standard is timely, putting risk management and mitigation front and centre.

PwC Australia is an advisor and a provider of assurance over controls to achieve compliance with prudential requirements. The effective performance of these roles in a way that is aligned with APRA's objectives requires that both we, and APRA-regulated entities, have clarity regarding the obligations and intent of the proposed standard. Thank-you for considering this submission. If you have any questions or would like to discuss any of our responses in more detail, please see our contact details below.

Yours faithfully,

[redacted]
Partner
e: [redacted]

[redacted]
Partner
e: [redacted]

# Executive summary

PwC Australia supports the introduction of APRA's draft Prudential Standard CPS 230 – Operational Risk Management (proposed standard) in Australia.

The Australian economy – and the community more broadly – relies on the ability of the financial services industry to operate uninterrupted. Therefore, it is imperative operational risk management lays at the heart of its critical functions, supporting the continuity of financial services to support Australia's modern digital economy.

Operational risk management will be key to drive APRA's desired outcome to improve operational resilience and minimise impacts of disruption to customers and the financial system. Operational resilience has been a topic of increased focus over the last decade globally, driven by a number of critical factors and events, including the COVID-19 pandemic, technological disruption, increased reliance on service providers (both business and technology) and significant operational incidents which have impacted business operations, customers and financial system stability. Globally, regulators are setting clear expectations that organisations should make the strategic shift from business continuity management (BCM), which is recovery focused, to more holistic management of end-to-end operational risk.

The introduction of Prudential Standard CPS 234 (Information Security), alongside existing standards CPS 231 (Outsourcing) and CPS 232 (Business Continuity), has established a strong foundation in driving operational resilience. This foundation will be further enhanced by the proposed standard.

We agree that the proposed standard will drive the following outcomes:

- Strengthening operational risk management: Improving how entities manage operational risk, ensuring they have a current and detailed understanding of their operational risk profile, are operating effective controls and, to the extent possible, preventing disruptions to their critical operations.
- Improving business continuity planning for critical operations: Developing adaptable processes, systems and capabilities to help ensure businesses better prevent, prepare for and predict disruptions, as well as build strong continuity capability to respond to, and recover from, disruptions within tolerance levels and drive continuous improvement.
- Enhancing third-party risk management: Expanding requirements to cover all material service providers relied upon for critical operations will continue to uplift resilience and enable consistency of expectations with shared service providers.

To support the successful implementation of the proposed standard, we have identified several key areas for further clarity and guidance. These include:

- **Operational risk management:** Updating of the term "material service" to "critical operation" under Paragraph 27 to align with the proposed standard. In addition, we suggest providing guidance on how to interpret the word "timely" under Paragraphs 29 and 30, to drive consistency across APRA-regulated entities.
- **Business continuity:** Guidance on how to identify critical operations and set appropriate tolerance levels. We also recommend the inclusion of training requirements in the proposed standard because it is an important component of business continuity - establishing critical 'muscle memory' that will carry employees through a response to a crisis or disruption.
- **Service provider management:** Further clarity on the service providers intended to be brought into scope, particularly those that manage information assets under Prudential Standard CPS 234 - Information Security. We also suggest that a minimum expectation for the monitoring of fourth parties be provided.

# Consultation responses

PwC has responded to APRA's consultation Questions 1, 2 and 8 from the Discussion Paper - Strengthening operational risk management.

***Question 1: Is a single cross-industry standard for operational risk management supported?***

PwC supports a single cross-industry standard for operational risk management. The proposed standard will drive consistency and standardisation in how risk and resilience is considered and managed across the banking, insurance and superannuation industries. A material weakness or incident impacting any of the APRA-regulated industries has the potential to threaten Australia's financial system stability. Given the objective of the proposed standard, as noted by APRA, is to minimise the impact of disruption to customers and the financial system, a common bar set across industries is important to success.

There are many instances where an APRA-regulated entity is considered a service provider to another, or a service provider is engaged by many different APRA-regulated entities. Therefore, a single standard will also enable consistency in the engagement and expectations of shared material service providers.

The Prudential Standard CPS 234 – Information Security is also a cross-industry standard. While we see differences in interpretation across APRA-regulated entities, a single standard has aided in the setting of a consistent expectation for all regulated industries, particularly as APRA and the assurance profession works through the CPS 234 tripartite reviews.

For any industry-specific considerations, this could be set out in a practice guide similar to Prudential Practice Guide CPG 234 Information Security.

***Question 2: Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?***

As outlined below, we have identified key areas where further clarity and guidance would support successful implementation of the proposed standard as well as assurance over the controls adopted to comply with the standard.

## Operational risk management

### Operational risk profile and assessment

Paragraph 27 requires the APRA-regulated entity to conduct a comprehensive risk assessment before providing a material service to another party. We note that "material service" is not a defined term within the standard and does not align with the rest of the proposed standard which refers to critical operation.

### Timely remediation of material weaknesses

Paragraph 30 states that "remediation must be supported by clear accountabilities and assurance, and address the root causes of weaknesses in a timely manner". We suggest further clarity be provided as to what is considered to be "timely" remediation. We have seen varying interpretations of what is considered to be timely remediation when assessing compliance with the Prudential Standard CPS 234 – Information Security. For example some APRA-regulated entities would determine timely remediation based on having a remediation plan and funding in place, even if this timeline spans across a number of years. Therefore, further guidance will support APRA-regulated entities in establishing processes for remediation of material weaknesses and drive further consistency across APRA-regulated entities.

Consideration could be given to harmonising these definitions across standards to provide greater clarity and consistency.

## Business continuity

### Identifying critical operations and defining tolerance levels

Guidance on how to identify critical operations and how to set appropriate tolerance levels will support APRA-regulated entities with the definition of these topics. This could be set out in a practice guide similar to Prudential Practice Guide CPG 234 Information Security.

### Absence of training

Prudential Standard CPS 232 – Business Continuity Management, clearly distinguishes between the requirement for periodic testing of the Business Continuity Plan, and the establishment of programs for training and awareness of staff in relation to Business Continuity Management. We recommend training is included in the proposed standard because it is an important component in a business continuity lifecycle, establishing critical 'muscle memory' that will carry employees through a response to a crisis or disruption.

## Service provider management

### Material service providers

A "material service provider" is defined as providing "a critical operation", and some of the examples included in Paragraph 49 include "funding and liquidity management" and "underwriting". As an example, it is unclear whether 'underwriting' is intended to refer to underwriting activities performed by investment banks, or insurance underwriting, or both. We note that the supporting CPS 230 Discussion Paper - Strengthening operational resilience refers to underwriting only under Insurance. Additionally, funding and liquidity management could be interpreted as capturing lending activities undertaken by banks, thus triggering the need for a comprehensive risk assessment for each lending transaction. We would suggest that further industry-specific clarity be provided for the examples provided under Paragraph 49, either in the proposed standard or in a practice guide similar to Prudential Practice Guide CPG 234 - Information Security.

### Critical and sensitive information assets

Paragraph 50 includes in the definition of material service providers those providers that manage "information assets classified as critical or sensitive under CPS 234". CPS 234 requires APRA-regulated entities to classify their information assets by criticality and sensitivity, and in practice many APRA-regulated entities have assigned a criticality and sensitivity rating for each information asset. As currently worded, this could mean in some scenarios that every service provider will be scoped in as a material service provider as there will be a criticality and sensitivity rating assigned to the information assets they manage, even if the rating is the lowest possible. We suggest further clarity be provided to better understand which service providers should be brought into scope under Paragraph 50.
In addition, the proposed standard aligns with CPS 234 in focusing on service providers (CPS 230) and related or third parties (CPS 234) who "manage information assets". We have interpreted "manage" to include those service providers/related and third parties who not only manage but hold, or have access to, an entity's information assets. This can and has been interpreted differently by APRA-regulated entities. We recommend that further guidance is provided to ensure consistency in application by APRA-regulated entities.

### External audit providers

We seek clarity on whether it is APRA's intention that the appointed external auditor is intended to be classified as a material service provider. The provision of financial statements audits and 310-related assurance reporting could be seen as a critical operation (Paragraph 48) and the external auditor would hold (and thus, depending on definitions, manage) information assets classified as critical or sensitive under CPS 234.

### Scope of management's regular assessment

Paragraph 47(d) states that the APRA-regulated entity's service provider management policy must include "the entity's approach to managing the risks associated with any fourth parties that material service providers rely on". We suggest that a minimum expectation for monitoring of fourth parties be provided. Given the extensive divergence of work performed to date regarding third parties, more detailed guidance on the expectations of fourth party monitoring could prevent a similar issue with the implementation of the proposed standard.

## APRA intervention

There are four paragraphs in the proposed standard (Paragraphs 36, 38 and 51, 54(b)), that include the provision for APRA intervention, or on-site visits, to a material service provider where needed. For example, Paragraph 38 states that "APRA may set tolerance levels for an APRA-regulated entity, or a class of APRA-regulated entities, where it identifies a heightened risk or material weakness". We suggest further guidance be given with respect to what would trigger such an intervention and how this would occur.

***Question 8: What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?***

APRA should consider implementing a 'transitional' period, similar to the one applied for the implementation of Prudential Standard CPS 234 - Information Security. This would mean APRA-regulated entities would be required to meet service provider management obligations with third-party providers at the earlier of contract renewal, or one year from the commencement of the proposed standard. This would serve to reduce the potential cost and compliance burden for organisations, and balance the need for the proposed standard to be fit for purpose, while enabling captured entities to focus on their core business.

www.pwc.com.au