Wednesday 19 October, 2022

To the General Manager, Policy, APRA,

RE: Proposed Prudential Standard CPS230 Operational Risk Management

The Australasian Chapter of the Business Continuity Institute (BCI) welcomes the opportunity to respond to the Australian Prudential Regulatory Authority's (APRA's) invitation to comment on its draft Prudential Standard CPS230 *Operational Risk Management* (CPS230). Banking, finance, insurance, and superannuation service providers are a critical part of every modern society. The BCI encourages its members and their organisation(s) to take all reasonably practicable steps to enhance societal security and resilience. APRA's revision and modernisation of prudential standards is an important activity we consider closely aligned to our organisation's values.

About the BCI

The BCI has been the world's leading institute for business continuity and resilience professionals since 1994. The BCI is the authoritative, reliable and global source of information on all aspects of Business Continuity theory and practice for professionals and those who have an interest in organizational resilience and provides a platform for industry experts and organisations to share best practices.

BCI Australasian Chapter CPS230 Working Group

The BCI Australasian Chapter (the Chapter) proposed to its members that a Working Group should be formed to:

- review the proposed CPS230 Standard and provide feedback
- submit feedback to APRA

The Working Group is comprised of 14 Chapter members who collaborated to undertake a review of CPS230. The Working Group members individually and collectively possess deep experience in disruption, continuity, and operational resilience. The members' collective work experiences include critical infrastructure, banking and finance, transport, energy, water, telecommunications, and technology/digital sectors. Several members of the Working Group will be responsible for guiding their respective organisation's practical implementation of the proposed CPS230.

We note that the employers of some Working Group members operate in or service customers in multiple regulatory jurisdictions which, in addition to Australia, include the United Kingdom, United States, European Union, Hong Kong, New Zealand and Singapore. Consequently, these members are also considering how to effectively implement operational resilience standards in different jurisdictions concurrently.

Disclaimer

This submission represents the view of the Working Group. It should be read in concert with similar submissions provided to APRA by APRA-regulated entities. This submission does not purport to represent the views of either the BCI or as a whole or any APRA-regulated entity either individually or as a collective.

Confidentiality

The BCI acknowledges APRA's policy to publish all submissions on the APRA website.

Context

The BCI Australasian Chapter CPS230 Working Group has reviewed the draft CPS230 and referred to the Discussion Paper: *Strengthening operational risk management* (discussion paper) published in July 2022. The BCI has not been briefed by APRA on the background and change drivers or the overall intent of CPS230. The draft CPS230 has been reviewed as that a business continuity practitioner may use to guide the design, implementation, management, governance, and compliance of an APRA-regulated entity's business continuity activities. Therefore, we welcome an opportunity to have BCI members briefed by APRA on the context and intent of the draft CPS230.

General feedback and recommendations

General recommendations following on from feedback from various BCI practitioners across Australasia and the Working Group propose with regards to CPS230, APRA may:

- Consider the impacts of the omitted detail from the consolidation of several standards into a single prudential standard e.g. removal of requirement for a BC policy, Business Impact Analyses, etc.,
- Describe the intent or definition of the concept implied by "*material adverse impact on … depositors, policyholders, beneficiaries or other customers,*"
- Seek to align more closely to applicable International Standards, the BCI's Good Practice Guide and the operational resilience standards currently under implementation in other jurisdictions,
- Provide clear requirements for management of critical service providers and reducing potentially unforeseen complexities during implementation,
- Provide detailed support in the form of a Prudential Practice Guide outlining what is expected as evidence of implementation of the new standard.

We recommend that APRA ensure definitions for key terms introduced in CPS230 are included in APS001 – Definitions.

We recommend that APRA consider the applicability of the Security of Critical Infrastructure Act 2018 (SOCI Act) and Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) to CPS230.

Specific feedback

In its Discussion Paper: *Strengthening operational risk management*[1], APRA posed eight questions to guide respondents' feedback on the overall design and specific requirements of CPS230. The Working Group's response to the eight questions is tabled as *Annex A - Response to consultation questions*.

The Working Group's detailed feedback and recommendations on specific topics and areas of guidance which may assist implementation is provided in *Annex B – Detailed feedback.* Our Working Group's feedback may be summarised as follows:

- Further clarification is required regarding definitions of terms, concepts and timeframes, or where APRA-regulated entities may use their own definitions,
- Language could be improved if definitions and descriptions aligned with that available in International Standards, such as:
    - ISO31000:2018 *Risk Management – guidelines*,
    - ISO22301:2020 *Security and resilience: Business Continuity Management Systems – requirements*,
    - CEN/TS 17091:2018 *Crisis management – guidelines for developing strategic capability,* and
    - globally recognised guidelines such as the BCI *Good Practice Guide*.
- Further detail is recommended in describing the relationship between Operational Risk Management, Business Continuity, and Service Providers,
- Further guidance in relation to implementation, with regards to the intent of APRA's use of material service provider lists and power to direct APRA-regulated entities use of such providers.

Conclusion

Thank you again for the opportunity to provide these comments. If you wish to discuss any aspect of this submission, please contact the Chapter at [redacted].

Kind regards,

[redacted]

BCI Australasian Chapter Lead, on behalf of the CPS230 Working Group

[1] APRA Discussion paper: *Strengthening operational risk management* Chapter 5 Consultation and next steps – Consultation questions

Annex A: Response to consultation questions

Overall design	***1. Is a single cross-industry standard for operational risk management supported?*** BCI supports a single cross-industry prudential standard.
	2. Are there specific topics or areas on which guidance would be particularly useful to assist in implementations? We have provided detailed feedback on specific topics and areas of guidance which may assist implementation in *Annex B – Detailed feedback.* Key points include encouraging the development of a Business Continuity Management Programme that includes a Policy, Business Impact Analysis, and Business Continuity Plans, and consideration for Crisis/Incident management. Consideration may also be given to existing international standards for guidance on definitions and best practices.
	3. *How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?* CPS230 describes *Critical operations and tolerance levels* as those undertaken by a regulated entity which, if disrupted, have a "material adverse impact on its [the regulated entity's] depositors, policyholders, beneficiaries or other customers". This implies that the focus is on the affected consumer and not the security of the financial system. Therefore, there should be no difference in requirements for an SFI and non-SFI as disruption of a non-SFI may have a material adverse impact upon that entity's customers. Less stringent requirements for non-SFI may be seen as a barrier to competition by an SFI.
	4. What are the estimated compliance costs and impacts to meet the new and enhanced requirements? The Working Group members expressed concern about the impacts of the requirements in CPS230. We expect that the Working Group members will consider this question in their employer's response to APRA. The Working Group considered a cost-benefit analysis to be out of scope for its submission.
Specific requirements	**5. How could APRA improve definitions of critical operations, tolerance levels and material service providers?** The term 'critical operations' is succinctly defined in Paragraph 34. The term 'material service provider' is contained in the second sentence of Paragraph 48. This definition should be moved and placed immediately after Paragraph 46. The term 'tolerance levels' does not have an adequate definition and should be explored in a prudential practice guide to be developed by APRA in advance of the proposed CPS 230 implementation date of 1 January 2024. While a definition has been provided in APRA's discussion paper, it is in the context of the entity and not the consumers experiencing the effects of a disruption to critical operations.

	6. What additions or amendments should be made to the lists of specified critical operations and material service providers? The list of critical operations and material service providers appears to contain sufficient guidance however may be too prescriptive. Paragraphs 35 and 49 imply that all regulated entities and APRA have a shared understanding of each term's meaning. Definitions for each should be provided The term 'customer enquiries' in Paragraph 35 requires clarification. The inclusion of internal audit in Paragraph 49 appears out of place as a service provider and is not stated or implied in Paragraph 35.
	7. Are the notification requirements and time periods reasonable? APRA should clarify the relationship Paragraphs 32 and 41. This comment is expanded upon in Annex B.
	8. What form of transition arrangements and timeframe would be needed to renegotiate contract with existing service providers [if required] The lens of what is reasonably practicable should be applied. New agreements reached on and after 1 January 2024 should comply with CPS230. The APRA-regulated entity should develop a timetable to identify where change is required and then implement that change to existing arrangements no later than 1 January 2027. Additionally, Paragraph 52. (c) should be expanded or a prudential practice guide provided to describe what minimum steps APRA considers reasonable and how the entity should respond to APRA's belief, based on data, that a service provider as systemically important.

Annex B – Detailed feedback

CPS230 Paragraph	Feedback
230.7	APRA should include in CPS 230 or in supporting documents, such as APS001, GPS001, HS001, 3PS001, definitions for terms including: *Critical operation* *Material adverse impact* *Material financial impact* *Material service provider* *Operational resilience* *Resilience* *Tolerance levels* The BCI has defined the following terms in the Business Continuity Institute Good Practice Guide 2018 which may provide a baseline for APRA's definitions: • *Critical* - A qualitative description used to emphasize the importance of a resource, process or function that must be available and operational either constantly or at the earliest possible time after an incident, emergency or disaster has occurred. • *Critical Operation(s)* - Those activities which must be performed to deliver the key products and services, and which enable an organization to meet the most important and time-sensitive objectives. • *Operational Resilience* - Ability of an organization, staff, system, telecommunications network, activity, or process to absorb the impact of a business interruption, disruption or loss and continue to provide an acceptable level of service. Definitions as described in other operational resilience standards around the world may also be considered e.g. UK Prudential Regulation Authority or Financial Conduct Authority (FCA).
230.11	Define *Severity* in the context of impact to the business and its customer. Recommend Critical Operations and Critical Service Providers are defined and identified through a Business Impact Analysis (BIA).
230.12	APRA should clarify the intention of Paragraph 12. We recommend amending 'processes or systems' to 'processes and/or systems,' to allow for the event an internal failure occurs at the same time as a failed system.
230.13	Recommend updating phrasing to "return to normal operations, or improvements to normal operations due to lessons learnt to reduce residual operational risks," to remove any contradictions between 'tolerance levels' and 'after the disruption'.

230.14	Recommend rephrasing to require if "an entity relies on a service provider, it must make every effort to ensure that it can meet its prudential obligations".
230.15	APRA should clarify if the risk management framework includes risk management policy, business continuity policy and service provider/outsourcing policy. APRA should define the frequency of “regularly” stated in requirement 15.(e).
230.19	APRA should consider clarifying the roles and responsibilities of the Board, and its relationship with APRA.
230.21	APRA should consider if requirements 21. (b) and (c) are reasonably practicable for Board members to have the level of involvement described, especially in the case where entities may have multiple BCPs and multiple corresponding service providers.
230.22	APRA should clarify when the Board should be informed. As written, the Paragraph suggests that such information would be provided on an as-needed basis to support a Board-level decision such as strategic investment.
230.24	APRA should clarify the term “appropriate and sound information” and consider replacing it with “relevant and accurate”.
230.31	APRA should reconsider the words “in a timely manner” and adjust the Paragraph to read: “An APRA-regulated entity must ensure that operational risk incidents and near misses are identified, escalated, recorded, and addressed in accordance with the entity’s risk management policy. An APRA-regulated entity must take all incidents and near miss data into account in its assessment of its operational risk profile and control effectiveness”.
230.32	APRA should clarify Paragraph 32 as it is currently unclear if the notification period relates to an incident which has been avoided or a situation where an APRA-regulated entity is proactively responding to a developing situation to avoid the financial impacts and/or adverse impact to critical operations reaching a material threshold.
230.39	APRA should consider amending Paragraph 39 as follows: (b) reword to read – “triggers to identify and assess the disruption, criteria for activating the plan, arrangements for directing resources to execute the plan, and tolerance levels required before de-escalating". (c) reword to read - “a list of required knowledge, skills, experience and resources necessary to support the effective implementation of BCP actions”.
230.42	APRA should consider enhancing Paragraph 42 and provide a stronger linkage to Paragraph 40. Recommend rewording to: "An APRA-regulated entity must have a documented annual testing program which uses a range of plausible severe scenarios to validate that all critical operations, including those performed by service providers, may be sustained within tolerance levels. Throughout the 12-month period, the entity must evaluate the effectiveness of its BCP and the capabilities of its senior managers to respond to disruption".
230.44	APRA should amend the review period from "on an annual basis" to "at least annually or after recovery from an incident reportable to APRA and completion of a Post Incident Review".
230.45	APRA should specify the term "periodically" and we recommend that this is established as "at least annually”.

230.47	APRA should consider the appropriateness for an operational document (register) being maintained within the policy. Requirement 47(d): Further guidance from APRA is required as to the minimum steps APRA considers to be reasonably practicable.
230.52	Requirement 52(c): APRA should provide in a prudential practice guide what reasonably practicable steps an APRA-regulated entity may take to meet this requirement. In the context of Paragraph 51, what data might APRA provide to assist an entity's due diligence? CPS230 Paragraph 52 appears to remove the obligation to consult described in CPS231 Paragraphs 39 and 40.
230.55	APRA should amend the requirement to become: "For each arrangement with a material service provider, an APRA-regulated entity must take all reasonably practicable steps to:".
230.56	APRA should define heightened prudential concerns and the timing of such requirement. CPS230 should define the steps that may be taken by an APRA-regulated entity to reduce the risk of such concerns being raised after a formal agreement with a new service provider has come into effect.