Deloitte.

Prudential Standard CPS 230
Operational Risk Management
Deloitte response to consultation

28 September 2022

Deloitte Touche Tohmatsu
ABN 74 490 121 060
Grosvenor Place
225 George Street
Sydney, NSW, 2000
Australia

Tel: +61 2 9322 7000
www.deloitte.com.au

Gideon Holland
General Manager, Policy
Australian Prudential Regulation Authority (APRA)
via email: PolicyDevelopment@apra.gov.au

28 September 2022

Dear Gideon

Deloitte response to consultation on CPS 230 *Operational Risk Management*

Please find enclosed the Deloitte submission in response to consultation on the draft Prudential Standard, CPS 230 *Operational Risk Management* (CPS 230).

Deloitte supports APRA's objectives and principles-based approach outlined within the discussion paper and draft Prudential Standard. We note that APRA plans to finalise CPS 230 in early 2023, for implementation on 1 January 2024. To support the development of the final standard, Deloitte welcomes the opportunity to provide feedback and have identified key principles and considerations based on our on global experience in this area and discussions with industry participants.

We welcome the opportunity to discuss and share our industry insights with APRA on this topic in more detail if required.

Yours sincerely,

Sean Moore
Partner, Risk Advisory
Financial Services Industry Lead, Australia
Deloitte Touche Tohmatsu

Caroline Brell
Partner, Risk Advisory
Financial Industry Risk & Regulation
Deloitte Touche Tohmatsu

Introduction

We welcome the opportunity to respond and provide feedback on APRA's industry consultation on the draft Prudential Standard *CPS 230 Operational Risk Management* (CPS 230). The update consolidates a series of existing standards, and is opportune in timing given the change in not only the regulatory landscape, but the industry itself.

It is against this backdrop of significant change that has re-emphasised the need to focus on operational resilience. Under the proposed draft Prudential Standard, regulated entities will be required to modernise their approach in understanding and managing operational risk, and in doing so, consider the impact CPS 230 will have on:

- **Critical Operations –** This is part of the evolution of how regulated entities will manage risk and third-parties with a focus on critical operations rather than the traditional service provider, product- or business-line basis. As the industry sharpens its focus on critical operations, the guidance provided by APRA to support the implementation of CPS 230 will play an instrumental role in assisting regulated entities to better understand and meet APRA's expectations in the lead up to, and post-implementation of CPS 230.

- **The Financial Services Ecosystem and potential for concentration of risks –** Certain associated parties hold a substantial proportion of data for the Financial Services Industry (FSI). This also extends to technical resources within their control; and notably, these parties generally operate outside of APRA's traditional regulatory scope (for example, superannuation fund administrators and technology providers).

- **The continued evolution and growth of the digital wave** – Technology continues to have an increasing impact on the FSI in terms of how regulators will look to address and adopt rapidly growing digital assets. Regulators have been paying, and continue to pay, close attention to the potential risks digital assets may pose, whilst also appreciating the potential of these assets to transform the operation of not only financial markets, but also how consumers engage with the FSI.

- **Cross-border implications** – The appropriate regulatory approach for parties operating or relying on entities outside of Australia is still yet to be determined. Many entities have operations or use service providers outside of Australia. The introduction of CPS 230 will have broader (and potentially new) cross-border implications, which are traditionally not viewed as within APRA's remit.

- **Regulatory fragmentation** – The introduction of the standard will introduce new and enhanced requirements for entities outside of APRA's regulatory remit, such as critical service providers to the FSI (for example, major technology providers). While regulators across the globe are aligned in their intent to strengthen operational risk management, differing approaches by regulators may give rise to challenges for firms that operate across multiple jurisdictions, with respect to managing both distinct and intersecting requirements.

In our view, the introduction of CPS 230 is a strong reflection of how APRA is seeking to deliver on its objectives outlined in their Corporate Plan for 2022-23, specifically with respect to the objective of modernising the prudential framework. A consolidated and principles-based approach to regulating operational risks will better facilitate practical implementation and ongoing compliance with the standard.

We note one of APRA's key priorities is to increase operational resilience across the FSI, and therefore our response focuses on:

- **Principles based regulation -** We believe that prescriptive supervisory measures may be counter-productive to the FSI's ongoing investment in enhancing their internal risk management capabilities and culture.

- **Alignment with better practice observed globally -** Global regulators are moving in parallel to strengthen operational resilience, particularly in light of recent geopolitical events that have challenged the assumed norms of the FSI. We have observed shared intentions between APRA's CPS 230 and recent regulatory updates, such as the recent draft of the Digital Operational Resilience Act (DORA) and the Critical Third-Parties Regime from the European Union (EU) and United Kingdom (UK), respectively. In our response, we have considered these recent changes in the global regulatory landscape, and have incorporated items that, in our view, reflect better practice for APRA's consideration.

- **The Financial Services ecosystem -** The introduction of CPS 230 will have broader implications beyond regulated entities. The expansion of the regulatory perimeter will prompt regulated and unregulated entities alike, to consider the maturity and adequacy of their existing operational risk management frameworks.

1 Response to Consultation

Our responses to the consultation questions are derived from our deep experience working with clients to understand and effectively implement regulatory change. In addition, through our experience, we have observed historical and persistent challenges that regulated entities have faced related to operational risk management.

1.1 Overall Design

Question	Deloitte Response
Is a single cross-industry standard for operational risk management supported? Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?	We support APRA's approach to introduce a single, cross-industry standard relating to operational risk management. Given the principles-based nature of CPS 230, we believe detailed guidance is required to support regulated entities to understand APRA's expectations with respect to implementation, and ongoing compliance with the new requirements. Given the dynamic and evolving nature of the FSI, this guidance should be updated on an ongoing basis, which will assist regulated entities to better respond to changes in their operating environment and regulator expectations as they arise. Guidance should consider outlining APRA's expectations with respect to how regulated entities and their critical service providers would meet and demonstrate compliance with the requirements of CPS 230. In our view, the language used in paragraph 11 of SPG 515 is an example of where APRA has provided a sufficient level of guidance, without prescription. In addition, to support practical implementation of CPS 230, we believe APRA should provide specific examples/guidance on: • We note that the role of the board as outlined in paragraphs 21-22 of CPS 230 represents heightened expectations and guidance to clarify how these requirements are expected to be met will be particularly pertinent to regulated entities; • The expected degree of comprehensiveness required for risk assessments (as specified in paragraph 27 of CPS 230), for example, if there is an expectation to conduct a vulnerability assessment as part of the overall risk assessment. Paragraph 16 of SPG 515 provides an example of the level of detail we have found regulated entities find useful; • Types of scenarios that may be considered 'severe but plausible'; • Tolerance levels; and • How regulated entities can appropriately determine the materiality of service providers to critical operations and apply the appropriate level of oversight, irrespective of where they sit in the value chain. For example, for fourth parties and beyond. In addition, guidance that provides examples of key metrics have been particularly helpful to assist regulated entities in implementing the requirements of Prudential Standards to APRA's expectations. For example, those outlined in prudential practice guides developed to support some of the more recently published, outcomes-focused prudential standards, such as Attachment A of CPG 234, SPG 515 and SPG 516.

Question	Deloitte Response
How could proportionality be enhanced in the standard, and is there any merit in different requirements for significant financial institutions (SFI) and non-SFIs?	We note that one of APRA's long term objectives is to incorporate proportionality to a greater extent within the prudential framework. In our view, the first approach outlined on page 14 of the CPS 230 discussion paper will be better received by regulated entities. The implementation of a set of requirements that are applicable to all regulated entities, and which are met by all entities (to the extent that it is commensurate with the scale and complexity of their business), is more in line with a principles- and outcomes-based approach to regulation. We are particularly conscious that an entity's operating model, is a key determinant of risks that entities are exposed to (for example, an entity that largely manages its critical operations in-house will have a different risk profile to an entity that manages its critical operations using third-party service providers). We note that with this approach, guidance to supplement principles-based regulation is critical, and will support entities of all sizes to form a view on the expected activities required to facilitate compliance with CPS 230, as well as to support robust operational risk management practices. The alternate (and more explicit) approach, which would see smaller, less complex entities not deemed to be SFIs exempt from complying with specific requirements, implies a more binary view of financial institutions (which often is not reflective of the current state of the FSI). As the FSI becomes increasingly interconnected, consequences of gaps in operational resilience will similarly follow this trend. This has become particularly pertinent due to an increasing concentration of service providers that the FSI share. We believe that prescriptive supervisory measures may be counter-productive to the FSI's ongoing investment in enhancing their internal risk management capabilities and culture.
What are the estimated compliance costs and impacts to meet the new and enhanced requirements?	Compliance costs associated with new and enhanced requirements will differ across the industry and sectors, and will greatly depend on current maturity levels of the respective organisations. Much of the FSI has already invested in uplifting regulatory compliance mechanisms in response to a marked increase in regulatory change in recent years.[1] In our view, it is likely that there will be implementation and on-going compliance costs for regulated and unregulated entities alike. Whether these costs are passed on or absorbed by the regulated entity will depend on several factors including, the operating environment, relative bargaining power and existing relationships with service providers. Furthermore, with respect to impacts of the new and enhanced requirements, we believe that these will be concentrated around those with data and technology implications as these areas historically require substantial financial investments and efforts from the business to implement. Many aspects of data and technology are heavily interlinked with external service providers, meaning that impacts on existing contracts will also be key. We believe that the proposed timeframe for the implementation of CPS 230 will be challenging for regulated entities, given the significant scope of uplifted and new requirements. In our view, APRA should consider extending the timeframe for full compliance with CPS 230 over a period of 2-3 years, on a similar basis to the extension of CPS 234 compliance which was implemented to account for third-party arrangements. We note that the impact of CPS 230 on both regulated and unregulated parties will be significant, and with the concentration of service providers to the FSI, an extended timeframe will better support compliance with new and enhanced requirements.

[1] Deloitte *Managing Regulatory Change in the Australian Financial Services Industry Survey* (May 2022)

1.2 Specific Requirements

Question	Deloitte Response
How could APRA improve the definitions of critical operations, tolerance levels and material service providers?	The scope of critical operations, tolerance levels and material service providers are broad and will differ based on the context of the relevant regulated entities. APRA should consider the following approach for these definitions: • **Critical operations –** The definition of 'critical operations' is currently focused on the delivery of services. APRA should consider reviewing and expanding the definition of critical operations to include operations that would materially impact or impair the regulated entity's ability to meet and comply with regulatory, financial and operational obligations on an ongoing basis, as well as systemic risks relevant to the broader FSI. • **Tolerance levels –** The proposed definition of tolerance levels in the draft Prudential Standard may be improved by providing: o Guidance for regulated entities to apply an industry specific lens; o Tolerances around operations critical to the financial, regulatory and operating performance of regulated entities; and o Increased scope to account for other/industry specific key considerations such as those that may result in detriment to customers, policy holders and members. For example, the Best Financial Interest Duty (BFID) in the case of Superannuation funds and other fiduciary obligations, as appropriate. Further, these tolerance levels should reconcile with the underlying risk appetite established by the regulated entities and be endorsed by the Board. This would in turn, facilitate how regulated entities are considering the impacts of operational risk, on not only the operations of the regulated entity, but also on other factors such as financial performance. • **Material service providers –** The current definition provided in the draft Prudential Standard is appropriately detailed.
What additions or amendments should be made to the lists of specified critical operations and material service providers?	APRA may also wish to consider incorporating guidance, or clarifying general terms. For example, clarification of the level for the terms 'mortgage brokerage' and 'insurance brokerage' used in paragraph 49. A distinction between the broker and aggregate level may improve interpretation and compliance with the standard.
Are the notification requirements and the time periods reasonable?	The draft CPS 230 currently specifies notification requirements across multiple sections. APRA should consider a similar structure taken for other prudential standards such as CPS 220 and CPS 234, that is, the inclusion of an explicit section for notification requirements.
What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?	We note new and enhanced service provider requirements within CPS 230 will be a key focus for both regulated and unregulated entities. Many regulated entities and service providers may take the introduction of CPS 230 as an opportunity to also review existing provisions during the contract review and renegotiation process. As these activities will be occurring across regulated entities, key service providers for the FSI will observe a simultaneous increase in requests, potentially resulting in capacity constraints. There is likely to be significant delays and protracted timeframes to completion across the FSI that will be exacerbated by a shorter implementation timeframe with limited transition arrangements.

2 Key Authors and Contributors

Sean Moore

Partner, Risk Advisory
Financial Services Industry Lead, Australia

semoore@deloitte.com.au

Caroline Brell

Partner, Risk Advisory
Financial Industry Risk & Regulation

cbrell@deloitte.com.au

Mike Ritchie

Lead Client Service Partner, Risk Advisory
Financial Services Industry Lead, Asia Pacific

miritchie@deloitte.com.au

Tommy Viljoen

Partner, Risk Advisory
Cyber Risk Strategy and Governance

tfviljoen@deloitte.com.au

Max Murray

Partner, Audit & Assurance
Governance, Regulation & Conduct

mamurray@deloitte.com.au

Tim Noad

Partner, Audit & Assurance
Governance, Regulation & Conduct

tnoad@deloitte.com.au

Jonathan Sykes

Partner, Audit & Assurance
Business Assurance

jonsykes@deloitte.com.au

Jaramie Nejal

Director, Risk Advisory
Financial Industry Risk & Regulation

jnejal@deloitte.com.au

Suleigh Huang

Senior Analyst, Risk Advisory
Financial Industry Risk & Regulation

sulhuang@deloitte.com.au

Arjuna Raj

Director, Risk Advisory
Financial Industry Risk & Regulation

arraj@deloitte.com.au

Deloitte.