AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY
1 Martin Place (Level 12), Sydney, NSW 2000
GPO Box 9836, Sydney, NSW 2001
T 02 9210 3000 | W www.apra.gov.au

JOHN LONSDALE
Chair

10 July 2023

OIA ID: OIA23-04674

Mr Jason Lange
Executive Director
Office of Impact Analysis
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Email: helpdesk-oia@pmc.gov.au

Dear Mr Lange,

CERTIFICATION OF APRA'S REVIEW *PRUDENTIAL STANDARD CPS 230 OPERATIONAL RISK MANAGEMENT*

I am writing to certify that APRA's development of *Prudential Standard CPS 230 Operational Risk Management* involved a process and analysis equivalent to a final Regulation Impact Statement (RIS).

I certify that the review has adequately addressed all seven RIS questions. The attached documents, consisting of APRA consultation papers set out how APRA has addressed these questions.

APRA has estimated that the introduction of the measure may increase costs for industry by $22.9 million per year, as set out in Table 1.

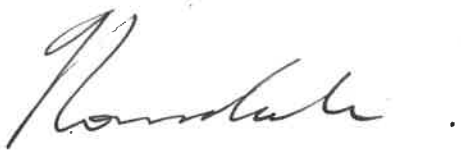
Table 1: Estimate of regulatory burden

Annual regulatory costs, averaged over 10 years $m				
Change in costs	Business	Community organisations	Individuals	Total change in costs
Total, by sector	22.9	0	0	22.9

A regulatory offset has not been identified. However, APRA is seeking to pursue net reductions in compliance costs and will work with affected stakeholders and across Government to identify regulatory burden reductions where appropriate.

Accordingly, I am satisfied that the attached report now meets best practice consistent with the *Australian Government Guide to Regulation*.

Yours sincerely



Attachments

Attachment A: *APRA Regulation Impact Analysis*

Attachment B: *Response paper, Operational Risk Management*, APRA, July 2023

Attachment C: *Discussion Paper, Strengthening Operational Risk Management*, APRA, July 2022

Attachment D: *Discussion Paper, Information Security Management*, APRA, March 2018

Attachment A: APRA Regulation Impact Analysis

Consistent with the Australian Government Guide to Regulation, APRA has followed a similar process to that required for a Regulation Impact Statement (RIS).

APRA has undertaken public consultation on the proposed operational risk management requirements and has engaged with a variety of stakeholders, including APRA-regulated entities and industry bodies. As detailed in APRA's June 2023 response to submissions, APRA has clarified or amended its proposals in certain areas, following consideration of issues raised by stakeholders.

In its July 2022 Discussion Paper, APRA set out the problem and why regulatory action was needed. In recent years, APRA-regulated entities have experienced operational risk events and failures that have had both financial and non-financial implications. APRA has observed three key trends: control failures, potential disruptions and increasing reliance on service providers.

APRA's policy development to enhance operational risk commenced in 2018 with APRA's proposal to introduce information security requirements for all APRA-regulated entities. The options outlined below reflect the original options considered when the project commenced in 2018. At that time, it was determined that information security requirements should be given first priority given the clear and pressing need to address the emerging issues in this area. As such, APRA adopted Option 2. The current policy development on operational risk management requirements reflects a continuation of that approach.

Policy options

Table 2: Options

Options	Approach
Option 1: Status quo	Continue with existing standards and guidance, relying on supervisory discretion to address any deficiencies in the risk management practices of entities.
Option 2: Stepped approach	Introduce prudential requirements on information security, ahead of other requirements on the qualitative management of operational risk management.
Option 3: Simultaneous approach	Introduce a prudential standard on the qualitative management of operational risk, which includes revised content on business continuity and outsourcing, and new content on information security.

Option 1: Status quo

Under the first option, APRA would continue with existing standards and guidance, relying on supervisory discretion to address any deficiencies in the risk management practices of entities. There would be no change in regulatory costs under this Option.

However, prudential risks would remain heightened. Without changes to the existing prudential framework, system-wide risks relating to operational risk, business continuity management and service provider management would not be reduced.

On balance, APRA considers there to be a long-term net cost associated with Option 1. While there are no additional regulatory costs associated with this option, there are long-term costs associated with the risks to financial stability and poor community outcomes.

Option 2: Stepped approach

Under Option 2, APRA would first introduce requirements on information security[1] and then introduce general operational risk management requirements[2].

Under this option, APRA-regulated entities would incur moderate additional regulatory costs. APRA estimates the cost to industry of the operational risk management requirements at an annual average of approximately $22.9 million over 10 years.

APRA's estimate is based on likely costs associated with updating policies, processes and frameworks, staffing costs and legal costs.

Option 3: Simultaneous approach

Under Option 3, APRA would have updated all relevant standards at the same time.

Under this option, APRA-regulated entities would bear the implementation costs of both sets of requirements simultaneously. Information security requirements would have faced a longer timeline than that under Option 2.

Assessment of net benefits

As outlined in APRA's June 2023 Discussion Paper, there are net benefits from APRA's approach to revising operational risk management requirements (Option 2):

- **strengthen operational risk management** with new requirements to address weaknesses that have been identified in existing practices of APRA-regulated entities. This includes requirements to maintain and test internal controls to ensure they are effective in managing key operational risks.
- **improve business continuity planning** to ensure that APRA-regulated entities are ready to respond to severe business disruptions, and maintain critical operations such as payments, settlements, fund administration and claims processing. It is important that all APRA-regulated entities are able to adapt processes and systems to continue to operate in the event of a disruption and set clear tolerances for the maximum level of disruption they are willing to accept for critical operations.
- **enhance third-party risk management** by extending requirements to cover all material service providers that APRA-regulated entities rely upon for critical operations or that expose them to material operational risk, rather than just those that have been outsourced.

In essence, the changes will help to ensure that APRA-regulated entities are resilient to operational risks and disruptions should they occur.

[1] Refer to Information security requirements for all APRA-regulated entities | APRA

[2] Refer to APRA consults on new prudential standard to strengthen operational resilience | APRA

Conclusion: Comparison of policy options

When developing policy, APRA is required to balance the objectives of financial safety and efficiency, competition, contestability and competitive neutrality, while promoting financial system stability in Australia.

While both Option 2 and Option 3 are similar, Option 2 has the additional benefit of giving priority to information security which is an area of heightened risk.[3] Therefore, APRA considered that Option 2 provides the greatest enhancement to prudential outcomes and improvement to financial system safety and stability in Australia.

Table 3: Comparison of options

	Option 1	Option 2	Option 3
Compliance cost	No change	Moderate cost	Moderate cost
Reduces system-wide risk relating to operational risk, business continuity management and service provider management	Does not meet this criterion	Meets this criterion	Meets this criterion
Considers local conditions	Does not meet this criterion	Meets this criterion	Meets this criterion
Prioritises higher risk areas	Does not meet this criterion	Meets this criterion	Does not meet this criterion
Overall	**(low) Net cost**	**Material net benefit**	**Moderate net benefit**

In summary, while Option 1 has a low net compliance cost, it does not convey the benefits of reducing risk for individual regulated entities or the financial system more generally, hence the lower cost comes with the risk of losses to customers as well as the potential for financial instability.

Implementation and review

APRA expects to release the final operational risk requirements in mid-2023, with effect from 1 July 2025.

As delegated legislation, prudential standards impose enforceable obligations on APRA-regulated entities. APRA monitors ongoing compliance with its prudential framework as part of its supervisory activities.

[3] *Prudential Standard CPS 234 Information Security* was finalised in in late 2018, with effect from 1 July 2019.