21 October 2022

General Manager, Policy
Australian Prudential Regulation Authority (APRA)
PolicyDevelopment@apra.gov.au

Dear General Manager

Submission on APRA's proposals to strengthen operational risk management (draft CPS 230)

We refer to APRA's Discussion Paper on strengthening operational risk management (the "Discussion Paper") and draft cross-industry Prudential Standard (CPS) 230 Operational Risk Management (the "Prudential Standard").

This letter sets out Riscentric's observations and responds to select APRA questions in the Discussion Note.

Riscentric's Observations

Riscentric launched in 2022 and specialises in Risk Management, with the sole focus of partnering with organisations that want to add value to their risk management activities. Having worked extensively in Risk Management at regulated entities, we support APRA's overall objectives and intent of a new Prudential Standard for operational risk management given how critical strong operational risk management is to achieving positive outcomes for the customers of regulated entities as well as the stability of the financial system. In particular, Riscentric supports:

- Responsibility for the oversight and management of operational risk remains with the business-line management (Line 1[1]) and not the risk management functions (Line 2[1] or Line 1 risk management functions). This distinction is often misunderstood within business-line management and is fundamental to risk management. Management of operational risk can only be achieved by the business-line with advice and challenge from the risk management functions.
- Senior management, as owners of operational risk, are required to provide clear and comprehensive information on operational risk to the Board, whose role it is to provide strong oversight of non-financial risks.
- APRA's comment that regulated entities are increasingly reliant on the use of service providers to support their business operations which requires broadening coverage of requirements from managing outsourcing to managing all service providers that the entity relies on.

Via exception, Riscentric's key observations on the Prudential Standard are:

Operational Risk Categories

APRA has provided a list of operational risk categories in paragraph 23 and stated that these sub-risks are 'including but not limited to'.

[1] Within the Three Lines of Defence model

Riscentric is of the opinion that providing a list of sub-risks could cause regulated entities to use this list instead of considering which are the most appropriate for their organisations. We would ask that APRA considers removing this list and including only the definition of operational risk in the Prudential Standard which will, in our opinion, allow entities to determine the appropriate sub-risk categories applicable to their organisation. However, if sub-risk categories are going to be included, then Riscentric requests that APRA consider the following edits to their list:

- While the risk of reputational damage is material to regulated entities, in our opinion, it is an outcome or impact of other risks e.g. cyber risk, fraud risk and we believe should not be categorised as a stand-alone sub-risk category.
- We note that APRA has categorised compliance risk, legal risk and conduct risk as operational risks and while we agree that they are non-financial risks, they do not, in our opinion, fall into the definition of an operational risk. A further differentiation is that we have observed Board's often have a lower risk appetite for these risks versus operational risks.
- We note that this list has omitted key operational risks including People risk and Fraud risk.

Control testing

APRA has stated that regulated entities must regularly monitor, review and test controls (paragraph 29). Riscentric strongly agrees with the intent of this statement but would point out that if this activity is not limited to testing only key control, it would be an extensive and costly activity for entities to comply with.

Responses to APRA's Questions

Riscentric has provided responses to select consultation questions below:

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

   Operational risk is generally industry agnostic and given the continued prevalence of operational risk incidents and failures across regulated entities, Riscentric supports the development of a single cross-industry standard for operational risk.

   While Riscentric acknowledges that different industries regulated by APRA are at different stages of risk management maturity, we support a single cross-industry standard for operational risk management to standardise requirements across all regulated industries. However, we believe that this will only work if as APRA has stated, regulated entities approach to operational risk is appropriate to their "size, business mix and complexity".

   In our opinion, a stand-alone Prudential Standard will also further signal to regulated entities the importance of uplifting their operational risk management practices with the aim and ultimate benefit of minimising loss and harm to customers and other regulated entities' stakeholders.

   Riscentric also believes the consolidation of CPS 231 and CPS 232 into a single prudential standard seeks to modernise APRA's prudential architecture. Given the synergies between these standards and operational risk overall, Riscentric is of the opinion that this consolidation will assist regulated entities to comply with these standards and has the potential to increase efficiencies.

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

The following areas would, in our view, be useful to receive further guidance on:

- *Paragraph 29 Control Testing:* As set out above, Riscentric believes that entities would benefit from further guidance on the scope of control testing required as a minimum.
- *Paragraph 47(d) Fourth Parties:* Riscentric agrees that significant risk can be introduced by fourth parties and supports the inclusion of fourth party risk management within the Prudential Standard. However, complying with this requirement may require significant changes to processes for many regulated entities and we expect that they would benefit from further guidance on the level of risk assessment required.

3. ***How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?***

Riscentric's view is that there is no merit in having different requirement for SFIs and non-SFIs as APRA has addressed this proportionality adequately in its opening guidance in the objectives of the Prudential Standard: 'an APRA-regulated entity's approach to operational risk must be appropriate to its size, business mix and complexity'. Differentiating the requirements for SFIs and Non SFIs may add further complexity to the prudential architecture and therefore we believe should be avoided.

4. ***What are the estimated compliance costs and impacts to meet the new and enhanced requirements?***

Riscentric are not able to provide estimated compliance costs but, at a high level, we would note the following additional costs:

- **Legal and compliance costs**: As legal and compliance advice will be needed to draft and potentially, renegotiate contracts with an expanded list of third parties (as set out in paragraph 48 and 53) as well as comply with the Prudential Standard.
- **Implementation costs**: Given the comprehensive nature of this regulatory change, we anticipate regulated entities will need to establish change and implementation programs at an extra cost with additional external resources or, at opportunity costs of internal resources (being diverted away from other work).
- **Assurance costs**: Significant additional cost could be created:
    - As each material service provider arrangement and contract will need to be reviewed by Internal Audit (paragraph 59).
    - APRA has stated that remediation of controls gaps and weaknesses must be supported by clear accountabilities and assurance and address the root causes of weaknesses in a timely manner (paragraph 30). Riscentric strongly agrees with the intent of a requirement to ensure that the root cause of weaknesses are addressed but would point out that requiring 'assurance', which traditionally can only be provided by Internal/External Audit (Line 3), would be a significant cost to entities.

7. ***Are the notification requirements and the time periods reasonable?***

Draft CPS 230 requires regulated entities to notify APRA no later than 72 hours after becoming aware of an operational risk incident that has a material financial impact. Riscentric notes that this notification requirement is not aligned with the provisions of the ASIC's Regulatory Guide 78. This misalignment may create additional costs and inefficiencies for regulated entities.

We trust the above observations and answers are of assistance to APRA.

We would be happy to elaborate on any aspect of this submission if that would be of use to APRA.

Yours sincerely

[redacted]
Founding Partner
[redacted]

[redacted]
Founding Partner
[redacted]