APRA CPS 230 – Operational Risk Management Consultation – GRCI Response

GRC INSTITUTE
GOVERNANCE • RISK • COMPLIANCE

General Manager
APRA
PolicyDevelopment@apra.gov.au

21.10.22

Thank you for the opportunity to provide input in regard to the draft CPS for Operational Risk Management.

GRCI members feel that this is an important piece of work and share the desire to achieve the objectives of greater governance and clarity in this area of business activity.

In our response we hope to particularly address the key questions APRA has asked around:
Notification requirements
Time periods
Transition arrangements and timeframes for renegotiation contracts with existing service providers.

In addition we have provided some insights into the guidance clarity that might be added to enhance the governance structures for operational risks within organisations, especially in light of APRA reporting requirements for incidents.
Our general observation is that some of the suggestions in the draft is not consistent with good 'three lines' hygiene or governance and better use of reference to the compliance risk function could be made to achieve the objectives of the guidance, particularly highlighting early involvement in supplier contract negotiations, remediation of incidents and alerts to incidents and BCP triggers.

If you have any questions at all about our input, please do not hesitate to reach out to us. We have recently reproduced a number of papers in regard to enhanced 'Three lines' operation to build more mature governance and accountability capabilities within organisations.

Kind regards,

[redacted]

[redacted]
CEO, GRCI

Key Feedback/Input

In order to achieve the objectives of the CPS GRCI suggests considering:

- Provide footnote for internal reference to the definition for "critical operations" – it is provided later in the document but is not italicised and so could be confused with an already defined term – so at least referencing in a footnote when it is first mentioned will draw attention to APRA's definition at Section 34 (and onwards.)

- Section 15 – a. Governance arrangements for oversight of operational risk is mentioned but thereafter there is a lack of consistency in advice/requirements to execute good governance by the omission of the role of compliance and risk professionals and their assurance activities. Further details are noted below where we consider the guidance should be adjusted.

- For example, after Section 30 there is an opportunity to acknowledge and overtly include the compliance function in the operational risk controls activities, especially in regard to remediation, especially as the CPS later requires an organisation to report to APRA. If the compliance function has previously been ignored in the governance structure for operational risk by the regulator themselves, then the entities are likely to do so as well and they then run the risk of the compliance function being sidelined and then surprised with needing to report to APRA and/or the report not being made in a timely manner.

- GRCI has raised this issue previously with APRA - the compliance risk function is the most likely to have to implement the regulatory changes imposed by APRA, even if it specifically outlines which function the requirements affect. The lack of acknowledgement by APRA within the guidance to include the compliance function fails to support APRA's previous comments on the necessity of the compliance function. To quote APRA's own website: "*Compliance risk has traditionally been the poor cousin of longer-established risks*"[1] There is a practical overlap between the requirements in this CPS and the role of compliance in the governance structure to ensure its effective execution. APRA would better support implementation if it overtly included reference to compliance risk here also.

- Similarly, Section 32 advises the reporting requirements but fails within the document to explicitly confirm the need to have the compliance risk function involved in the governance structure.

[1] https://www.apra.gov.au/news-and-publications/how-to-manage-compliance-risk-and-stay-out-of-headlines

- Query to Sections 36 and 38 about implementation timelines for the inclusion of additional business operations and tolerance levels to critical operations. GRCI anticipates that this would be advised at the time of APRA giving this direction but we thought it worth mentioning that, undertaking the requirements as per the draft CPS is a time consuming activity which will require dedicated and additional resources and a sensible timeline. We are sure is consistent with other feedback APRA will have received in regard to this CPS, so we would highlight the need for APRA to be prepared in advance to consider practical implementation timelines when adding defined critical operations.

- Query on Section 41 in regard to the 24 hour timeline giving consideration to the business week. While an entity would understandably respond over a non business day period to a BCP triggering event, would APRA really obtain value from having reporting provided if that event occurred over the weekend? We suggest APRA give consideration to a credible timeline guidance otherwise it can be difficult for compliance risk professionals to get traction in their organisations where the typical response might be "they won't even be looking at it over the weekend". Compliance risk professionals have the same level of interest in the success of the CPS as APRA does, but need clarity and credibility to back them up if need be. Some reference to business day operations would suffice.

- Query on Section 43 – will there be some further guidance provided around timeline and reporting expectations for when APRA does require the inclusion of an APRA-determined scenario in a BC exercise?

- Query Section 45 – again an interpretation of this section might lead an organisation to believe that the compliance risk function should not have any assurance role and thus enable an organisation to sideline them from the dialogue which would be a flaw in a comprehensive governance structure for operational risk.

- Service provider arrangements in sections 46 onwards will be problematic and complex to implement and members have strongly suggested a longer timeline to allow for this. As APRA would be aware, some supplier arrangements may not be currently comprehensively included in a whole of entity or group governance structure with compliance risk oversight at any level. The implementation timeline currently being required, in some entities, would not be enough time to execute to the level of maturity that would bring benefit to the entity and the market. GRCI members suggest 18 – 24 months minimum.

- In particular the Section 53 requirements will, in themselves, take some time to renegotiate and might compel organisations to change providers if they will not agree to the requirements. This will significantly delay the activity and could also pose a risk to the very operational elements APRA is seeking to ensure organisations are managing.

- Section 53 e in particular may be legally challenging to negotiate and enforce.

- Query regarding Section 54 – this will also be difficult to negotiate but GRCI would also question whether APRA has the resources, or wishes to invest in the resources and expertise, to be able to assess the documentation, data or on-site visits or whether this will just become an additional expense for APRA and its regulated entities with no particular benefit obtained. It seems likely in our estimation, that it will simply result in consulting firms being contracted to undertake this work and increasing their profits without noticeably improving the governance of operational risks from either a market or regulatory perspective. APRA needs to consider whether this realistically provides value as it will be likely be one of the most difficult elements to negotiate with service providers in the Australian market, particularly if they are multinational providers and there is no equivalent Australian provider or there is a lack of competition in that provider space.

- It might provide greater value if an entity had to otherwise substantiate the governance structures they had established to manage these risks than on-site visits or data will ever provide. There is also the added risk for the suppliers, entities and the suppliers' other customers of the potential for unanticipated risks to IP and privacy, from this kind of scrutiny.

- Again, as previously mentioned, Section 59 does not include overt consideration of the role of compliance risk in the review of proposed outsourcing arrangements. We are uncertain why APRA would ask a third line function to undertake a second line activity in the proposal stage. For the three lines to work effectively the third line would review after the second line. In the scenario described in Section 59, the compliance risk function would likely be independent enough to conduct the review and advise without compromising the governance of the operational risk. The organisation then has the opportunity for gaining further assurance from a third line review of the process from proposal through to execution and thereby both the market and the entity obtain better value and assurance.