

Neil Grummitt
General Manager, Policy Development
Policy, Research and International
Australian Prudential Regulatory Authority
GPO Box 9836
Sydney NSW 2000
Via email: riskmanagement@apra.gov.au

19 February 2014

PRINCIPAL MEMBERS



Dear Neil,

The GRC Institute would like to thank APRA for providing an opportunity for us to comment upon the draft prudential practice guide for CPG 220.

GRCi is the peak industry body for the practice of compliance, risk and governance in the Asia Pacific region. Our members are compliance, risk and governance professionals who are actively engaged in the private, professional services and Government sectors.

Overall the GRCi is supportive of the CPG 200, however there are a few minor but specific comments we would like to make that we believe would improve clarity for APRA regulated entities.

Firstly, we believe that the expectations that APRA have for CROs and the risk management function is much clearer than for the compliance function. We believe that the same clarity can be achieved if similar guidance, that is currently contained within Paragraph 65 around the structure and reporting lines of the compliance function, is also introduced into paragraph 56, so that various compliance roles within the organisation are placed with the correct business context and any ambiguity around reporting can be removed.

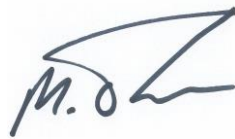
Additionally we believe that the Three Lines of Defence Model contained within Appendix A could also benefit from providing additional clarity around the role played by compliance. In fact for this to be a more effective model and truly represent the manner in which this model was created, it should be referred to as the Three Lines of Defence Risk & Compliance model, as both components are required if this is to be truly an effective tool for regulated entities.

| | | | |
|-----------------------------|-------------|-----------------|-----------------|
| Level 1, 50 Clarence Street | Australia | +61 2 9290 1788 | +61 3 9229 3871 |
| Sydney, NSW, Australia 2000 | Hong Kong | +852 3125 7665 | |
| ABN 42 862 119 377 | New Zealand | +64 9 363 2749 | |
| www.acigrc.com | Singapore | +65 6322 1463 | |

Having said this, Appendix A needs to ensure that the "independence" elements of the model are clear. For example, while a risk or compliance manager with a major division of the business maybe independent of the individual business units, these roles may not be able to achieve independence from the division, unless they are able to report to more senior managers that the divisional manager reports into. Having the compliance and/or risk functions reporting directly into these divisional managers has the potential to call this independence into question.

Once again GRCi would like to thank APRA for providing an opportunity for us to make comment on CPG 220. Should you require any additional information or require clarification on the comments that appear in this submission please do not hesitate to contact GRCi on +612 9290 1788.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'M. Tolar', with a stylized flourish extending to the right.

Martin Tolar CCP
Managing Director

Please note that the views expressed in this submission represent those of the collective GRCi membership. Consequently, individual members and organisations may hold a different perspective on some of the points raised and therefore reserve the right to make comment in their own right.