Royal Commission into Misconduct in the Banking, Superannuation, and Financial Services Industries

25 October 2018

Submission on the Royal Commission Interim Report

PRINCIPAL MEMBERS

Thank you for the opportunity to provide comment to the Royal Commission's Interim Report.

The GRC Institute is a membership based organisation for compliance and risk professionals throughout Australia, New Zealand and Hong Kong. Our members work for a variety of organisations both within financial services and much wider.

GRCI began in 1996 as the Association for Compliance Professionals of Australia, we have partnered with regulators and other parties to create the world's first compliance standard: AS/NZS 3806 and then took this to the International Standards Organisation to develop it to ISO 19600. Our members' in depth understanding of how to facilitate compliance throughout organisations and the stumbling blocks to achieving best practice has often been wasted in organisations where there is little understanding of how it can best work and often, unfortunately for our members, senior management and the board dictate reporting paths and resources that unintentionally contradict their stated desire for their organisations to be compliant.

Our submission has been put together based on our years of experience with our members' working in a variety of organisations and their feedback on their experiences with building compliance frameworks and education programs to assist them with being compliant and providing positive outcomes for their organisation's customers. We will attempt to be practical and constructive in our response to this draft and provide insights from our members' experience, successes and failures.

General feedback:

Our first observation is that the use of the term 'compliance' and 'compliance schemes or frameworks' throughout the whole of the testimony of the Commission has demonstrated clearly that both regulators and the regulated continue to struggle to understand how a compliance framework can be

Australia +61 2 9290 1788
Level 1, 50 Clarence Street
Sydney, NSW, Australia 2000
ABN 42 862 119 377
www.thegrcinstitute.org

utilised, who should perform that work, who they should report to and the responsibility of business to be accountable for compliant conduct, rather than continually expecting it to be 'done by someone else' – presumably in the back office, fixing all their mistakes.

This has not been surprising to GRCI or our members. It has been the frequent experience of our members that compliance and compliance professionals are under resourced, not utilised correctly in organisations, placed in the wrong positions in the structure of the organisation and should very definitely have a clear reporting line to their boards and protections if they need to go directly to the regulator.

Although a logical connection, compliance obligations and the framework to facilitate compliant behaviours throughout the organisation, do not simply form a subset of a broader risk management framework. That is just one *perspective* that is essential for an organisation to be across its obligations, however, often those undertaking and reviewing the risk framework overall may forget to apply alternate perspectives: such as the risk to reputation, customer, the risk *of* an incident as opposed to managing and assessing the potential consequences *to the organisation* if an incident occurs.

It is critical that governments, regulators, industry/professional bodies, trainers, auditors etc need to accept and understand that governance, compliance , risk, assurance, continuity is the role, responsibility and accountability of the Board, Senior management, middle/front line management, supervision and workforce both collectively and individually not the specialist/professional engaged by the organisation such as compliance officer/manager, risk manager etc. Their role of the professional (compliance/risk manager) is to facilitate, guide etc those with the responsibility to carry out their job to the standard required.

The role of the specialist or CO (Compliance Officer) professional is to put their hand up when something is wrong. If management or the board will not cause the issue to be investigated and remediated, including customers appropriately compensated in a reasonable time period then there should be a statutory requirement for the CO to discuss with the regulator. The CO would use the usual channels first - ie management first - board audit or risk committee chair. The CO would need to be a recognised position and candidates formally approved by APRA and ASIC. ASIC and APRA would need to have approved the education, skills and experience requirements for such COs.

Compliance professionals have a specific skill set and knowledge base that enables them to *facilitate* the understanding and uptake of suitably compliance conduct within organisations. If allowed to fulfil their role, unobstructed, compliance professionals work with business to understand in practical terms what the law and regulations require of them and how that applies to the products they develop, sell and manage with their customers. The business is the 'first line' – they conduct themselves in a compliant manner - which includes best interests of the customer – through the facilitation of the compliance professionals in their organisation. However it is vital that organisations understand that the 'first line' includes senior management and the board. They too must understand and embed compliant conduct and action it themselves.

The 'second line' is compliance, acting as a business compliance and conduct facilitator. They can't be *in* the business units or report to business units as they need clear reporting to the board and CEO but the facilitate the creation of compliance business systems, policies and processes, undertaken by the business for themselves with the assistance of the second line. Compliance professionals should ideally have protections offered should they feel it necessary to go to a regulator with an issue if the board or senior management refuses to take appropriate action.

The 'third line' is audit, whose vital checks are necessary. Audit should also have a clear line of reporting and similar suggested protections to go the regulator if necessary. Compliance professionals and auditors should not be considered ordinary whistleblowers and their protections should be absolutely clear.

Specific observations throughout the Interim Report:

Product suitability:

GRCI would suggest that there are disconnects in product development and that the regulatory approach should remain principle based, rather than adding more and more specific regulation. New products are continually developed and with technology changes the rate of development will continue. Applying principle based regulation to the process of product development, in law, that can be applied to any future developments should assist and if there appear to be the requirements for targeted regulation it can be assessed at that time. Our suggestions would be:

Have agreed definitions around complexity of products, customer risk assessments and other risk areas for customers that dictate who it can be sold to, how it can be sold, and other parameters.

Compliance professionals should be required to be an active part of the product development to facilitate the product developers/business understanding the nuances of requirements and conduct expectations around the product **as** they develop it, not a set of rules applied afterward. Many issues could be circumvented easily in the first place. Again, compliance should not report to this area of the business or product development and should be able to report arising issues directly to the board if they are observed.

Products should require a regular 360 degree review after implementation to ensure there aren't any unanticipated risks arising, that the product is both being sold and used as intended.

Piecemeal compliance:

The Interim report frequently mentioned the piecemeal application of compliance. Our observation would be that this often arises because of the misplacement of the compliance professionals in organisations but, quite essentially, it is also because **regulation is developed in a piecemeal fashion.**

GRCI is very definitely not opposed to regulation! However, in practical terms, there are many, many pieces of regulation developed in response to arising issues in the market and then applied like multiple band aids on organisations. This does not help the development of more holistic and principles based compliance frameworks. It can be distracting from proper conduct issues and creates confusion in organisations.

This is not the fault of regulators or compliance professionals, however it obviously doesn't help matters! It is not the additional regulation per se – which is obviously intended to assist – but it would be worthwhile returning to first principles and taking stock of the underlying issues, much as the Royal Commission has, to return to core messages and clear repetition. We would suggest that matters should not need to get to the point of needing a Royal Commission for this to occur however.

Observations of greed and poor conduct:

This is essentially the heart of the issue and has been a recurring theme in many industries, not just banking, for centuries.

Our observations from the Interim Report, testimony and experiences outside is that there are a number of missing elements for success:

- Compliance and conduct KPI's should apply to senior management and directors and they should not be able to be removed by shareholders. Although it should be part of the governance remit, the financial success of the organisation is seen as the overriding measure. Indeed, shareholders have, in the past, voted to remove compliance KPIs from a bank CEO's contract because it brought the shareholders no return on investment.
- Directors are inadequately equipped in many instances, to ask compliance and risk management questions with any depth of knowledge. They often know the industry very well and focus on the same performance measures they may have had when working within that organisation. Directors in particular need assistance from compliance professionals and/or additional training.
- Compliance needs to be able to report directly to the board and/or the regulator in the case of an issue arising. It should not be only reported internally to be 'risk assessed'. The Corporations Act is quite clear regarding 'suspected breach' requirements and boards need this level of information to do their jobs appropriately.
- There needs to be both the 'carrot' and the 'stick'. Senior management and directors need to be able to be held accountable with much more suitable penalties that are enforced. And they should be rewarded for ensuring the best conduct occurs in their organisations. Incentives work (as the Royal Commission has observed) but we need to reward the *right* behaviours.

This submission has been compiled from GRCI member feedback. GRCI and their members are both capable and willing to be the facilitators and governance advisors for helping the financial services industry to regain trust and community respect. Our members are Compliance Professionals who believe in and take pride of their vocational call to instil good corporate governance in both financial services and non-financial services sectors.

We would love to discuss our submission further, should you have any questions we can be contacted directly via our Sydney office.

Kind Regards,

[redacted]

Naomi Burley
Managing Director
GRCI