HERBERT SMITH FREEHILLS

ASIC CORPORATE GOVERNANCE TASKFORCE: DIRECTOR AND OFFICER OVERSIGHT OF NON-FINANCIAL RISK REPORT

09 October 2019 | Australia
Legal Briefings – By **Priscilla Bryans** and **Jessica Ginberg**

The ASIC Corporate Governance Taskforce (**Taskforce**) released its 'Director and officer oversight of non-financial risk report' (**Report**) on 2 October 2019. The Report follows the review by the Taskforce of director and officer oversight of non-financial risk in financial services companies, and is based on a sample size of just seven.

Although the Taskforce's review has been limited to a handful of APRA regulated companies, ASIC expressly states that its findings apply to all ASX listed companies.

The Report does not contain any 'surprises'. The themes it covers repeat many of the observations arising out of the APRA Prudential Inquiry into the Commonwealth Bank of Australia (**APRA Report**) and the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report (**Royal Commission Final Report**). It largely focuses on compliance risk and board oversight of internal risk management processes. The Report reflects a snapshot in time, relating to the companies' practices in 2017 and 2018. ASIC encourages Directors to read the full Report.

The Report is divided into three sections: risk appetite statements, information flows and board risk committees (**BRCs**). Our key observations on each section are set out below.

RISK APPETITE STATEMENTS

ASIC's key concern in this section of the Report is: "How do directors and officers use risk appetite statements to oversee non-financial risk in their companies?"

Key themes	ASIC's concerns	Our observations
Do we have a risk appetite statement and is it meaningful?	**Boards can do more to express their appetite in a way that is meaningful and aligns with their actual risk appetite.** The Report notes: • one company, which sought to measure when it was approaching appetite limits used an 'early warning' level and 'intervention' level which indicated when it was outside appetite; and • another included statements describing the company's expectations when non-compliance did occur (e.g. expected process for identifying, escalating and remediating breaches).	Boards should approve the risk appetite statement as it relates to non-financial risks (rather than simply receiving or noting it) – when they actively engage in the approval process, they have a greater stewardship of the non-financial risk appetite.
Are metrics measuring non-financial risk providing a full picture to the board?	**Risk appetite and accompanying metrics for non-financial risk were "immature" compared to those for financial risk.** Metrics should not only focus on actual breaches. Metrics designed to measure risk often failed to provide a representative sample to the board of the level of risk exposure, and did not allow accurate benchmarking to the board's stated appetite. Boards should require management to undertake "root cause" or thematic analysis to identify underlying causes of recurring breaches. Emerging risks also need to be assessed.	The board should receive reporting on metrics that enable the board to easily assess whether the entity is operating within risk appetite for non-financial risks. Directors need to understand the metrics and how they relate to the risk appetite statement. We expect listed companies will need to spend time identifying leading (as well as lagging) indicators of non-financial risk and developing appropriate metrics to have a full picture of existing and emerging non-financial risks.
What is required when a company falls outside its risk appetite statement?	**ASIC observed management "operating outside of board approved risk appetite for non-financial risks, particularly compliance risk".** The Report refers to multiple examples of "tacit" acceptance of boards, some "for years at a time", as well as boards not operating in accordance with charters.	If management is operating outside the approved risk appetite statement for non-financial risks, minutes should demonstrate that the BRC is actively seeking to urgently return the company within its appetite. It is not enough for the board to express its disappointment. The board must consider corrective action or, alternatively, whether the risk appetite statement should be amended because it does not truly reflect the entity's appetite. Recurrent issues should not simply be dealt with as they occur. Where issues are recurrent or serious, boards should step back and consider compliance risk exposure holistically and prioritise the resolution of root causes.

INFORMATION FLOWS

ASIC's key concern in this section of the Report is: "Are boards getting the right information to enable them to oversee and monitor non-financial risk management?"

Key themes	ASIC's concerns	Our observations
Is management providing the board with the adequate quantity and quality of information?	**Board packs are too dense and voluminous**, making it unclear whether their primary purpose is to: • inform directors in the most effective manner; or • absolve reporters from exercising judgment as to what information should be omitted. **Boards need to take ownership of the information they are receiving and actively seek out adequate data** or reporting that measures or informs them of their overall exposure to non-financial risks. Boards should require reporting from management that has a clear hierarchy and prioritisation of non-financial risks.	ASIC has reiterated the existing law that boards are responsible for ensuring that they receive adequate information to make informed decisions. Echoing the concerns of the Royal Commission Final Report, ASIC is alert to not only the quantity of information received by the board, but ensuring that it is the *right* information. The Report emphasises the importance of managing the volume of documents and expressly drawing out material issues. We would add that, **board papers should be not only about the 'what', but importantly, the 'why'.** Information provided to the board should include both data and analysis. If management provide facts without analysis, precious time at board meetings will be spent conducting analysis, rather than allowing the board to use that time to test and challenge the analysis to ensure it is sound.
Avoiding asymmetry of information between board members	**Informal meetings should be conducted in a manner that avoids asymmetric information between board members** Non-executive directors often communicate with one another and management verbally (e.g. in discussions over dinner or in camera sessions without management). Board committees do not always report back to the full board adequately. This creates an asymmetry of information between various board members. Material information should not be lost in undocumented closed sessions.	ASIC has drawn the conclusion that informal meetings risk resulting in an asymmetry of information unless care is taken. As evidence of this, ASIC points to the fact that informal sessions are frequently not minuted. ASIC states that verbal updates may not be adequate and they do not result in a corporate record of the matters discussed. Clearly it is important that all directors are adequately informed of information material to the company and its risk management framework. Similarly, when the board makes a decision, that decision must be documented. When the board makes its decision on an issue, the directors should cast their minds to those matters considered outside the board room and whether or not they contributed to the overall analysis. If so, have they also been raised before the whole board, and should they be recorded formally in the minutes. However companies should not read the Report to mean that all informal discussions must now be recorded, nor that every director must be present for every discussion.
What level of detail is required in board minutes?	**Positively, ASIC has expressly endorsed the Joint statement on board minutes (August 2019) prepared by the Governance Institute of Australia and Australian Institute of Company Directors.** However, ASIC expresses concern that: "There was little evidence in minutes of directors actively engaging with the substance of proposals submitted by management or information reported to them, in terms of offering alternative viewpoints or driving action by management."	The debate about board minutes, and the level of detail they should go into, is clearly a focus for ASIC. **Some of the adverse comments ASIC made about particular minutes suggested ASIC may expect more detail than the joint statement (and case law) says is required.** In the recent APRA v IOOF case Jagot J said: "… the minutes of a meeting are not required to record everything that was said … minutes are not expected to be complete transcripts of words spoken at the meeting and nor do they need to record arguments for or against resolutions … It follows that the absence in the minutes of a detailed record of discussion or consideration about matters before the board does not support the conclusion that such discussion or consideration did not occur."[1] Boards and company secretaries should think carefully about the advantages and disadvantages of including additional detail in their minutes.

BOARD RISK COMMITTEES

ASIC's key concern in this section of the Report is: "How do directors and officers use board risk committees – in practice – to oversee non-financial risk in their companies?"

Key themes	ASIC's concerns	Our observations
Is the BRC meeting enough?	**BRCs should meet more regularly and spend more time on non-financial risk.** BRCs should devote enough time and be actively engaged to oversee material risks in a timely and effective manner. ASIC observed that, in relation to the financial services entities covered by the Report, where a BRC meets quarterly, it will have limited ability to respond to leading indicators in a timely manner or monitor time sensitive issues.	We expect that non-executive directors (particularly in the financial services sector) will find themselves spending more time on non-financial risk issues going forward. This may take the form of more frequently scheduled meetings (e.g. at least once every two months) or longer BRC meetings, or both.
Who should attend BRC meetings?	If all directors are invited to, and regularly attend BRC meetings, boards should consider their motivations for establishing such a practice. **ASIC recommends that in such cases, the board should consider making all directors members of the BRC, with voting rights.** If most, but **not all**, directors attend BRC meetings, ASIC sees a risk that BRC reports to the full board may become less fulsome, resulting in one or two directors having an asymmetry of risk information.	We expect that the practice of all directors attending risk meetings will grow (particularly in the financial services sector). If such companies follow ASIC's recommendation to make all directors members of the BRC, this has at least one significant upside. Many directors are finding that the board meetings spend so much time on compliance matters, it is detracting from their ability to focus on strategic issues facing the Company. By having all directors attend as members of the BRC, board meetings may be freed up to allow more reflection on strategic issues.
Is the BRC providing the board with the adequate quantity and quality of information in its reports?	**BRC reporting should be improved.** Reporting of BRC to the board should be more fulsome.	It is incumbent on the chair of the BRC to summarise key matters dealt with and discussed in BRC meetings when reporting to the board. Above, we observe that management should not provide the board with facts, unless they are accompanied by analysis. Similarly, reports to the board on the activities of the BRC should include not only a factual summary of what was considered, but also an analysis of the BRC's conclusions.

APPLICATION TO BROADER CORPORATE AUSTRALIA

When launching the Report, ASIC Chair James Shipton confirmed that ASIC no longer sees its role as only a conduct regulator. ASIC is increasingly taking a supervisory role, with the "aim of identifying problems before they become breaches."[2] APRA-regulated entities are already familiar with the concept of having a supervisory regulator, but this may be a new development for companies in other sectors.

Mr Shipton noted that inputs by behavioural experts (organisational psychologists) placed in the boardroom during the process were "very beneficial". While Mr Shipton does not propose to do so on an "ongoing basis", it seems from this comment that it is likely ASIC may use behavioural experts again.

It appears that ASIC views the APRA Report and the recommendations in the Royal Commission Final Report as 'essential reading', reflecting standard governance expectations (on par with the ASX Corporate Governance Principles and Recommendations and APRA's prudential standards).

As expected, ASIC has picked up themes that overlap with the APRA Report, including:
- prioritisation of non-financial risk;
- measuring performance/progress with respect to non-financial risk;
- adequacy of information sought by/provided to directors on non-financial risk; and
- adequacy of information flow between board Committees.

ASIC acknowledges the difficulty in identifying a non-financial risk. While there is a relatively good understanding of that term within the financial services sector, there is less clarity outside the financial services sector as to what the term means. The Report adopts a definition of non-financial risk which is aligned with the definition in the APRA Report, but adapted to cover more than just prudential institutions.

It captures:
• **operational risk** – the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events and includes legal risk but excludes strategic and reputational risk
• **compliance risk** – the risk of legal or regulatory sanctions, material financial loss, or loss to reputation an organisation may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards and codes of conduct applicable to its activities; and
• **conduct risk** – the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employee. It doesn't appear to focus on broader issues such as strategic risk.

In ASIC's opinion, there is room for significant improvement in board oversight of non-financial risks, and currently such oversight is "less mature than needed", although some directors and officers are starting to think laterally and innovatively to overcome non-financial risk management challenges.

The Report includes questions that ASIC believes boards of all large ASX-listed companies should ask themselves. These questions are replicated in **Appendix 1**. ASIC makes it clear in the Report that "there is no one size fits all solution" to its findings. Therefore boards should see these questions as another tool available to them when self-assessing.

This Report is the first of two reports that ASIC will publish in relation to the Taskforce's review of governance practices in corporate Australia. The second report will focus on Director oversight of remuneration practices amongst a selection of ASX 100 entities. This separate report is due to be released 'in the coming months.'

Appendix 1: A further break down of the report and the board questions

ENDNOTES

1. *APRA v Kelaher* [2019] FCA 1521 at [142].

2. "Launch of ASIC's report on director and officer oversight of non-financial risk", keynote address by ASIC Chair James Shipton, Sydney 2 October 2019.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PRISCILLA BRYANS
PARTNER, MELBOURNE
+61 3 9288 1779
Priscilla.Bryans@hsf.com

QUENTIN DIGBY
PARTNER, SYDNEY
+61 2 9322 4470
Quentin.Digby@hsf.com

ANDREW EASTWOOD
PARTNER, SYDNEY
+61 2 9225 5442
Andrew.Eastwood@hsf.com

REBECCA MASLEN-STANNAGE
CHAIR AND SENIOR PARTNER, SYDNEY
+61 2 9225 5500
Rebecca.Maslen-Stannage@hsf.com

TONY DAMIAN
PARTNER, SYDNEY
+61 2 9225 5784
Tony.Damian@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2021

SUBSCRIBE TO STAY UP-TO-DATE WITH LATEST THINKING, BLOGS, EVENTS, AND MORE
Close

© HERBERT SMITH FREEHILLS LLP 2021