Australian Institute of Company Directors

ASIC Corporate Governance Taskforce

Director and officer oversight of non-financial risk report, October 2019

Executive summary

1. Overview

The ASIC Corporate Governance Taskforce report on director and officer oversight of non-financial risk was released on 2 October 2019 at the AICD's Essential Director Update in Sydney, and can be accessed here.

ASIC's report examines corporate governance practices at seven large financial institutions, identifying "important shortcomings" in relation to the oversight and management of non-financial risk. The entities involved in the review were ANZ, AMP, CBA, IOOF, IAG, NAB and Westpac.

In particular, ASIC highlights deficiencies in entities' articulation of, and adherence to, risk appetite statements (particularly as they relate to compliance risks); information flows to the board; and functioning of board risk committees.

ASIC's report follows APRA's Prudential Inquiry into the Commonwealth Bank and the subsequent self-assessments of financial services institutions, as well as the final report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (see our summary here).

ASIC's findings are consistent with the inquiries that have come before it. It builds on the call for boards to enhance their oversight of non-financial risk, emphasising the need for boards to exercise "active stewardship", seek out adequate management reporting and actively engage with the information available to them.

Notably, ASIC's report indicates that the regulator will place great stock on minutes that evidence active board oversight of management, and calls for additional detail of key discussion points and reasons for decisions to be included (referencing the AICD and Governance Institute of Australia's joint statement on board minutes, which can be accessed here).

The report also includes a discussion of ASIC's views on "better practice" in relation to relevant governance practices, and sets out a number of questions for directors of large ASX-listed companies to ask (extracted in Appendix 1 to this paper).

It is important to note that the Taskforce's review has been undertaken at a time when boards of financial services entities in particular are closely considering their governance practices and grappling with oversight of non-financial risk. The report is a constructive examination of governance practices at a point in time, but market practice is continuing to evolve as boards focus on strengthening their approaches to their oversight role. As ASIC Chair James Shipton notes, "while many boards and companies have started addressing these issues, they appear to be at an early stage. Rectifying these issues requires immediate and sophisticated responses from companies and boards that will need to be prioritised".

Attached to the report is a separate independent report by Kiel Advisory Group that considers how behaviour and behavioural dynamics between boards and management can influence oversight of non-financial risk.

This paper sets out:

- high-level implications for directors (**section 2**);
- key findings and insights on risk appetite statements (RASs) (**section 3**);
- key findings and insights on information flows (**section 4**);
- key findings and insights on board risk committees (BRCs) (**section 5**);
- ASIC's suggested questions for boards of large ASX-listed companies (**Appendix 1**); and
- a summary of the independent report on the influence of board mindsets and behaviours on effective non-financial risk oversight (**Appendix 2**)

2. Implications for directors

Effective oversight of non-financial risk is undoubtedly front of mind for directors.

While the report reflects the governance practice of a select number of large financial services entities, all boards (particularly of listed companies) should consider ASIC's findings, and the scope to improve their own practices.

This is an important time for governance in Australia, with regulators increasingly focused on the role of the board in providing effective stewardship of their organisations, and willing to set out more detailed expectations of directors than ever before.

In brief, the report makes clear ASIC's expectations that:

- boards engage in greater challenge of management and do all they can to ensure that they receive the right information to oversee and monitor non-financial risk;
- directors exercise active stewardship which requires active probing and analysis of information presented by management, and judgment on the merits of proposals and the adequacy of management actions;
- boards take a more active role in overseeing non-financial risk, including taking a robust approach to the organisation's risk appetite statement and associated metrics;
- boards monitor the implementation of governance frameworks, focusing on substance rather than form; and
- directors actively consider whether they have capacity to dedicate adequate time to their roles in light of other board roles and commitments.

3. Risk appetite statements: misalignment between practice and statements

Key findings

- Risk appetite and accompanying metrics for non-financial risk were immature compared to those for financial risk;
- Management was operating outside board-approved risk appetites for non-financial risk for months or years at a time;
- 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; and
- Board engagement with the RAS was not always evident.

ASIC insights

ASIC notes that a RAS can be an effective tool for overseeing risk but calls for:

- ***Boards to hold management to account when companies are operating outside appetite*** - Too often, management was operating outside of board approved risk appetite statements for non-financial risks, especially compliance risks (sometimes for months or years at a time). ASIC calls for boards to do more to return companies to within appetite, and to require management to undertake root cause analysis to determine underlying causes of recurring breaches of RASs.

- ***Full board engagement with the RAS*** - Board engagement with risk appetite statements was not always evident. In one case, an entity did not include compliance risk appetite as part of its RAS, while in only two cases did metrics exist which measured whether entities were approaching compliance risk appetite.

- ***Careful consideration of metrics used to monitor non-financial risk*** – The metrics observed for compliance risk often measured discrete issues or areas of compliance, rather than providing insight into broader compliance behaviour. ASIC highlighted that:

    - Metrics should include leading and lagging indicators – for example, reopened internal audit issues or breaches of internal policies as precursors to breaches of the law (ie a "near misses" approach); and

    - Boards should reflect on how their metrics for non-financial risks (which varied significantly across the sample set) compare to metrics used to measure more mature non-financial risks such as WHS in mining and construction companies.

- ***Meaningful board reporting that shows how the company is operating compared to its risk appetite –*** Management should report to the board with meaningful data that shows how the company is operating compared to its risk appetite. By way of a "good practice" example, ASIC points to one company's compliance reports that showed how it was operating against its compliance risk appetite, including "risk mapping" that identified deteriorating trends in certain compliance categories to give the BRC advance warning of potential increases in compliance risk levels.

4. Information flows: quality not quantity

Key findings

- Material information about non-financial risk was often buried in dense, voluminous board packs – boards did not own or control the information flows from management to the board to ensure material information was brought to their attention;
- Management reporting often did not identify a clear hierarchy or prioritisation for non-financial risks;
- Care needed to be taken to ensure undocumented board sessions and informal meetings between directors didn't create asymmetric information at board level; and
- Information flows between board committees and full boards were sometimes informal and ad hoc.

ASIC insights

Consistent with commentary from Commissioner Hayne in the Financial Services Commission final report, ASIC stresses the importance of boards getting the "right" information to enable them to oversee non-financial risk management and hold management to account.

Its observations on information flows included that:

- ***Material information should not be buried in lengthy board packs or reports*** - Material non-financial risks were often buried in dense, voluminous board packs (average BRC papers ranged from 137 to 703 pages in length). ASIC asserts that:
    - directors need to be proactive in requiring management to deliver information in a form that will help them discharge their oversight mandate, with chairs in particular needing to engage with approaches to reporting; and
    - management reporting should have a clear hierarchy for non-financial risks that prioritises their importance. ASIC points to an example of "better practice" being a compliance report that provides detailed commentary on specific risks, ranked in order of greatest to least severe.
- ***Material information should not be lost in undocumented closed sessions*** – ASIC expresses concerns around closed sessions and action items not being formally documented/minuted (on the basis that it can lead to reduced or impaired information flows to the wider board or management who must address the issues raised), and suggests that this practice be revisited.
- ***Minutes should include key discussion points and reasons for decisions*** - Minutes were often brief and formulaic, preventing ASIC from determining the quality of active board oversight. ASIC suggests that boards review their practices against the AICD and Governance Institute of Australia joint statement on minutes (accessible here).
- ***Asymmetric information between board members should be avoided*** - Material information obtained through informal meetings should be disseminated to the full board, and information flows between the BRC and full board as well as between committees should be reviewed to ensure they are effective. ASIC notes that organisations that invited all NEDs to BRC meetings appeared to have less detailed reporting to the full board, on the basis that NEDs attend all the BRC meetings (which was not always the case).

5. Board risk committees: need for stronger, more timely oversight

Key findings

- 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. While minutes are not the sole source of evidence of the extent of directors' stewardship, the minutes reviewed would not on their own support an argument that directors were exercising active stewardship;
- The timing and frequency of BRC meetings was generally modest considering they are the board's 'workhorses' in relation to risk;
- Material risk issues were often escalated in an informal and unstructured manner outside regular committee meetings; and

- There is a trend toward full board attendance at BRC meetings (instead of a subset of board members). However, directors were rarely made formal members of the committee, creating the risk of disenfranchising board members through lost voting rights, and entrenching reduced information flows to the full board.

ASIC insights

ASIC addresses the vital role that BRCs can play in supporting boards to oversee risk and encourages all large listed companies to consider whether creating a dedicated BRC would benefit their long term interests. ASIC also points to the use of management level non-financial risk committees to raise the visibility of risks and in doing so assist the board in their oversight of them

The report suggests that there is clear scope for BRCs to improve their effectiveness, especially with regards to non-financial risk. Further:

- ***BRCs need to meet often enough to oversee risks in a timely manner*** – ASIC expresses concerns around limited sitting time of BRCs considering their mandates and the challenges faced by entities (total annual hours for BRC sittings ranged from 10 to 37). The report also notes that meeting agendas were largely set at the beginning of the year and were often dominated by standardised or repetitive items.

- ***Cross-committee information flow should be formalised*** - some organisations still appeared to rely on cross-committee membership as a key part of their information flows. ASIC suggests better practice includes minuting of key issues addressed by board committees that are automatically referred to other committees.

- ***Directors who sit on or chair BRCs should consider whether they are committing sufficient time to BRC-related duties*** – ASIC notes that directors who chair BRCs often sit on multiple company boards, and suggests that directors consider whether their number of roles allows them to discharge their duties effectively.

- ***There is a need for transparent and consistent processes for escalating urgent material risks outside committee meetings –*** ASIC expresses concerns about dealing with time sensitive matters (that are sufficiently material to be escalated to the BRC) in an ad hoc manner, and encourages companies to adopt transparent and consistent processes.

- ***The practice of all board members attending BRC meetings should be carefully considered*** – ASIC acknowledges both the advantages and risks, including reduced information flow to the full board due to the assumption that all board members will attend the BRC meeting.

To access ASIC's full report, click here

For further information or to share your thoughts, please contact the AICD team at policy@aicd.com.au

Appendix 1 - ASIC's suggested questions for boards of large ASX-listed entities

1 Risk appetite statements

1.1 Should we default to the position that the company should be operating within the board's stated appetite in the ordinary course of business?

When we fall outside appetite, are we requiring management to do everything within their power to return the company to within appetite, or otherwise cease activities that place it outside appetite?

1.2 Do I understand why our compliance risk appetite has been articulated in the way it has, and why certain metrics have been chosen (to the exclusion of others) to measure compliance risk?

1.3 Does our stated compliance risk appetite reflect our actual appetite? If not, what is the purpose of stating the appetite in this way and how will it help us oversee this type of risk in practice?

1.4 Are the metrics we have approved sufficiently representative to provide a picture of what we are trying to measure across the organisation?

1.5 Do our metrics allow us to measure performance against our articulated appetite?

1.6 Are we measuring non-financial risk in a way that provides us with early warnings of rising risk levels?

1.7 How do our compliance risk metrics and other non-financial risk metrics compare to those metrics used to measure financial risk; for example, for credit or liquidity risk?

1.8 Does management report to the board against the metrics in the RAS? Do management committees receive reporting against the metrics in the RAS?

2 Information flows

2.1 Is the breadth and materiality of information we are receiving from management correctly calibrated to help us perform our oversight function? Is the information we receive on non-financial risk of a similar quality to that we receive on financial risk?

2.2 Are significant issues receiving sufficient prominence in reports? Does management reporting make it easy to identify the materiality of non-financial risk across the organisation?

2.3 How are we ensuring that board members not present during closed sessions are informed about material non-financial risks? How are action items coming out of closed sessions recorded and conveyed to the board and management?

2.4 Do our minutes adequately capture key discussion points, reasons for decisions, and significant issues raised with management?

2.5 How are we ensuring that all directors have the benefit of material information obtained during informal conversations or meetings?

2.6 Are the methods we use to update the full board sufficient to ensure it receives reliable and timely information about material non-financial risks?

2.7 How robust are our processes for cross-committee information sharing?

3 Board risk committees

3.1 Are we dedicating sufficient time to risk issues, including non-financial risks at the BRC level? For BRC chairs: Am I allocating sufficient time to perform my duties as BRC Chair, taking into account the scale and complexity of the company?

3.2 Does the BRC meet often enough to oversee material risks in a timely manner? Does the frequency of our BRC meetings allow for the timely elevation of material risks to the committee?

3.3 Are we receiving the right kind of information to discharge our duties? How are we satisfying ourselves that this is the case?

3.4 Are we demonstrating active oversight of, and engagement with, matters being put to the BRC? Do we require management to act where we are not satisfied with what is being presented or recommended to the board?

3.5 Do we have transparent and effective processes for escalation of urgent material to the board? Are these processes followed consistently?

3.6 Are all board members (whether or not they are formal members of the BRC), fully informed, and do they have an opportunity to participate and be heard on risks? Is the BRC the right size to be effective? Does the BRC's charter accurately reflect the BRC's actual practice?

Appendix 2 – Report on influence of board mindsets and behaviours on effective non-financial risk oversight

Overview

Attached to ASIC's report is a separate independent report by Kiel Advisory Group that considers how behaviour and behavioural dynamics between boards and management can influence oversight of non-financial risk. The report can be accessed here.

The subject of significant media interest in the lead-up to its release, the report identifies behaviours and dynamics that the firm believes can help or hinder effectiveness in board oversight of non-financial risk.

It also outlines a number of board "archetypes", along with their strengths and weaknesses, with a view to supporting self-reflection and driving improvements in inter and intra board dynamics.

Scope of review

The review involved 19 listed entities from across both the financial services and non-financial services sectors.

In addition to targeted documentation review, the review was based on limited data including eight meeting observations (five board meetings and three board committee meetings), 35 confidential discussions with directors and senior executives, and 287 anonymous surveys completed by directors and senior executives.

Headlines

- The review found that the majority of boards exhibited the following common characteristics that helped rather than hindered effective oversight of non-financial risk including:
    - ***Directors displayed a self-concept centred on integrity both individually and collectively*** - there was an understanding of expectations and significant emphasis on ethical role modelling; and
    - ***Directors made conscious attempts to challenge management*** – including employing a range of strategies that demonstrated efforts to test management including "light touch" questioning, requests for additional information or analysis, disagreement with ideas or status of controls.
- The report also expresses views on "unhelpful" mindsets and behavioural norms noted including:
    - ***Difficulties engaging in genuine self-challenge*** – including as a result of limited time for unstructured discussion; framing decisions through a "functional prism" only; strong belief in the board's role and the business's moral compass that made it difficult to accept failings; and the use of language to downplay uncomfortable issues;
    - ***Attempts to resolve conflicting agendas*** – the report recognises that the role of the board is multifaceted but refers to implications for supervision and monitoring of non-financial risks including insufficient debate and challenge; and

- ***Difficulty understanding the business in enough depth to identify gap's in management's perspective*** – including where directors have not worked in the relevant industry on a day-to-day basis.

Implications for better practice

The report also suggests implications for better practice and considerations for boards, emphasising that skilled navigation of the group dynamic is a key differentiator of effective boards (ie individual capacity and preparedness is not sufficient).

It highlights a number of considerations for boards including:

- ***The need to improve ownership of their oversight role*** – including taking responsibility for creating an environment of transparency, accountability and collective oversight; and considering their own blind spots;
- ***Clarifying and focusing on outcomes rather than on processes*** – requiring a focus on the outcomes the board seeks to achieve through the processes of supervision and monitoring and ways to support these outcomes;
- ***Increasing their commitment to collective rather than individual performance*** – by focusing on collective functioning as least as much as individual performance;
- ***The need for chairs to take steps to mitigate risks inherent in their board's particular "style"*** – requiring an understanding the culture of the board and its impact on effectiveness; and
- ***A greater focus on informal drivers of effectiveness*** – such as understanding how to overcome natural interpersonal responses and challenges within a group.