ASIC
Australian Securities & Investments Commission

Corporate Governance Taskforce

Director and officer oversight of non-financial risk report

Contents

ASIC Report 631
Publication date: October 2019

Foreword

The reality is that non-financial risks have very real *financial* implications for companies, their investors and their customers.

The review by the ASIC Corporate Governance Taskforce into Australia's largest financial services companies has highlighted important shortcomings in corporate governance practices in large listed entities. In particular, oversight and management of non-financial risks has generally not received sufficient attention until recent times – in stark contrast to the focus on financial risk and financial returns.

Boards cannot afford to ignore the oversight of non-financial risks. We have seen first-hand the damage that can result when it is not made a priority. Mismanagement of non-financial risks in the banking and wealth sector has resulted in institutions announcing hundreds of millions of dollars in customer remediation costs. Industry analysts have also projected remediation costs and increased spending on risk and compliance in the sector in the billions of dollars.

Boards must recognise that they are accountable for mitigating all risks – financial and non-financial – facing a company.

Our Corporate Governance Taskforce was established with special funding from the Australian Government, following revelations of significant corporate governance failures during the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Financial Services Royal Commission).

We deliberately targeted large firms with the expectation that they should have mature procedures and the highest standards of governance and accountability in relation to non-financial risks.

Instead, our review revealed that boards were grappling with important elements of the management and oversight of non-financial risk – some more so than others – and their oversight was less mature than needed.

However, the review also observed that institutions increasingly recognise that they need to change past practices to minimise the likelihood of future failings.

Positively, we observed some directors and officers starting to think laterally and innovatively to overcome such challenges. Overall, the companies and their boards we reviewed need to significantly improve their practices to address the issues outlined in this report.

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.

We urge boards of all listed companies – whether or not you are in financial services – to read this report. Review your governance practices and accountability structures with reference to our findings, particularly that:

- All too often, management was operating outside of board-approved risk appetites for non-financial risks, particularly compliance risk. Boards need to actively position themselves to hold management accountable to operate within their stated appetites.

- Monitoring of risk against appetite often did not enable effective communication of the company's risk position. Boards need to take ownership of the form and content of information they are receiving to better inform themselves of the management of material risks.
- Material information about non-financial risk was often buried in dense, voluminous board packs. It was difficult to identify key non-financial risk issues in information presented to the board. Boards should require reporting from management that has a clear hierarchy and prioritisation of non-financial risks.
- Companies generally sought to use board risk committees (BRCs) to achieve desired outcomes, but their effectiveness could be improved. BRCs should meet more regularly, devote enough time and be actively engaged to oversee material risks in a timely and effective manner.

While there is no 'one size fits all' solution to these findings, boards need to proactively identify and assess their own characteristics and processes. This includes promoting the oversight of non-financial risk.

James Shipton
ASIC Chair
October 2019

Executive summary

Good corporate governance in the financial services sector is essential for a fair, strong and efficient financial system for all Australians.

The Financial Services Royal Commission highlighted significant shortcomings in the corporate governance practices of many large financial services firms listed on the Australian Securities Exchange (ASX), including in relation to the oversight and management of non-financial risk. ASIC has also been concerned that corporate reporting on governance has suffered from a 'form over substance' approach, with an emphasis on frameworks and processes rather than actual practices.[1] For example, in 2018, the published corporate governance statements of some companies subject to our review stated that they had the frameworks and processes required by the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*.[2] However, self-assessments into governance, accountability and culture, and the Australian Prudential Regulation Authority's (APRA's) prudential inquiry into the CBA[3], found governance practices in relation to risk to be wanting.

In August 2018, ASIC received funding to conduct targeted reviews of corporate governance practices of large listed companies to shine a light on actual governance practices. In its first year, ASIC's Corporate Governance Taskforce reviewed director and officer oversight through the lenses of non-financial risk and discretionary decision making in variable executive remuneration. (A report on executive remuneration practices will be published in the coming months.)

This report sets out our observations on director and officer oversight of non-financial risk. The seven financial services institutions selected for this review are those that many Australians are exposed to, through their personal and business banking, superannuation or insurance, or as shareholders.

The Taskforce's work

The Taskforce wanted to understand how directors and officers of these large and complex companies are discharging their duties in relation to oversight and monitoring of non-financial risk, and highlight ways to improve governance practices. It did not set out to conduct whole-of-company reviews; rather, it focused on governance practices at the highest levels of each company.

The review was largely structured around discussions with key members of management and directors of the relevant companies, and review of documents. We conducted 60 interviews with executives and directors of the seven companies included in this review, and received more than 29,000 documents.

1 See the ***Review of the ASX Corporate Governance Council's Principles and Recommendations – Submissions of ASIC***, Public Consultation on the Fourth Edition, 1 August 2018; and the ASX Corporate Governance Council's ***Corporate Governance Principles and Recommendations***, Fourth Edition, February 2019 (ASX Corporate Governance Principles and Recommendations).

2 **ASX Corporate Governance Principles and Recommendations**.

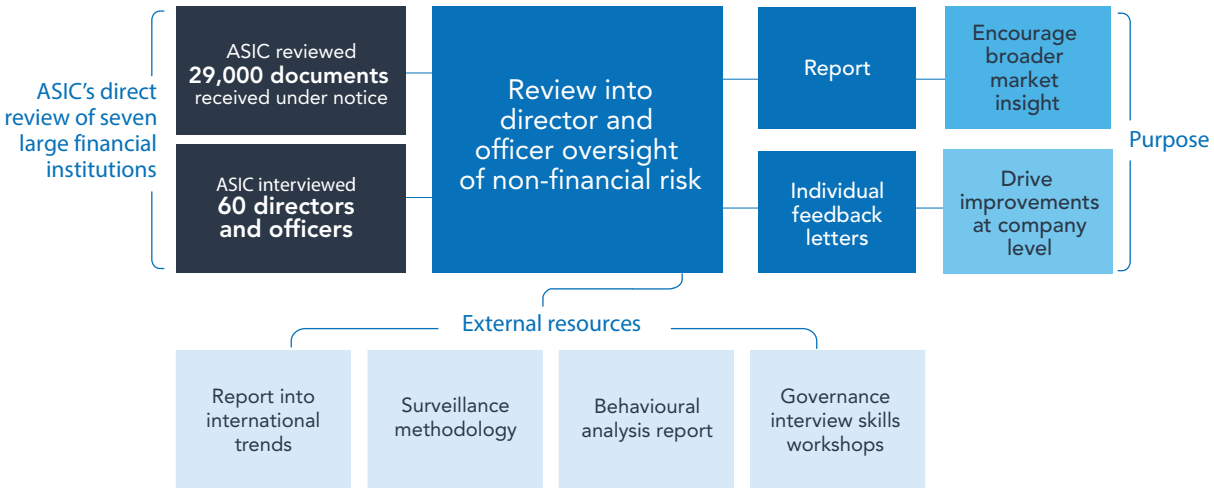
3 APRA, ***Prudential Inquiry into the Commonwealth Bank of Australia***, April 2018 (APRA CBA Inquiry Report).

We commissioned work from external firms to assist in our review, including Deloitte Touche Tohmatsu (Deloitte), who assisted us in developing our surveillance methodology (see Appendix 2). Deloitte also provided research into international governance practices relating to director and officer oversight of non-financial risk in the United Kingdom, the United States, Canada and Germany. This research identified global trends in governance practices that we used to inform our 'international trends' sections.

ASIC engaged Ms Pru Bennett, an expert in investment stewardship, to conduct a series of workshops with members of the Taskforce regarding interview techniques specific to discussions with executives and directors on issues relating to corporate governance.

We commissioned Kiel Advisory Group to independently review how behaviour and behavioural dynamics between the board and management can impact effective oversight of non-financial risks. This particular review is intended to assist boards in identifying their own behaviours. It can be used as a tool by boards to assist in overcoming some of the challenges identified in our review.[4] Throughout this report we highlight those matters that are also discussed (from a behavioural perspective) in the Kiel Advisory Group report.

ASIC's Corporate Governance Taskforce



4 Attachment A: ***Influence of Board Mindsets and Behaviours on Effective Non-Financial Risk Oversight***, Kiel Advisory Group, 2019 (Attachment A).

What we found

Many directors identified challenges with overseeing non-financial risks in large, complex organisations. Nevertheless, there was no strong, corresponding trend of directors actively seeking out adequate data or reporting that measured or informed them of their overall exposure to non-financial risks. Fractured or informal flow of information up to the board and around the board table meant that some boards did not always have the right information to make fully informed decisions. Where information did make its way to the board, there was little evidence in the minutes of some organisations of substantive active engagement by directors.

Some companies lacked awareness of the underlying issues, heightening deficiencies in practices. Other companies had acknowledged the scale of remediation efforts required, and executed initiatives to address governance shortcomings highlighted over recent years. This report refers to some of these initiatives as well as good governance practices we observed throughout our review.

We also observed that companies often had frameworks and structures in place to support board oversight of non-financial risk; however, in practice, deficiencies arose in compliance with, or execution of, these frameworks. For example, boards approved risk appetites that were intended to articulate the level of risk acceptable for company operations, but management operated outside this appetite for years at a time with the board's tacit acceptance. We saw boards approving charters governing the operation of BRCs; however, the boards did not hold themselves accountable to operating in accordance with those charters.

Specific findings

We considered how **risk appetite statements** (RASs) were being used as a tool to assist boards in overseeing and monitoring non-financial risk. We observed that:

- 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
- board engagement with the RAS was not always evident.

We reviewed **information flows** from management to the board and from board committees to full boards. Our review found that:

- 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
- information flows between board committees and full boards were sometimes informal and ad hoc.

We looked at the operation of **BRCs** and found 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. 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.
- 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.

Application to large ASX-listed companies

This report focuses on the practices of large listed financial services companies. ASIC, like the ASX Corporate Governance Council, believes that:

> **Different entities may legitimately adopt different governance practices, based on a range of factors, including their size, complexity, history and corporate culture.**[5]

The observations in this report are made with an understanding of this principles-based, rather than prescriptive, approach.

We recognise that companies outside the financial services sector often face different and unique non-financial risks; however, it is wrong to suggest that only the boards of financial services companies should make non-financial risks a priority. The observations and insights in this report can be applied across sectors. We urge the boards of all large ASX-listed companies to read this report and ask themselves the questions posed throughout. For ease of reference, we have listed the questions in Appendix 1.

5 ASX Corporate Governance Principles and Recommendations.

Regulatory basis for the Taskforce's review

One of ASIC's core responsibilities is to monitor, oversee and enforce directors' and officers' duties, as set out in s180–184 of the *Corporations Act 2001* (Corporations Act). These include duties to act with due care and diligence, in the best interests of the corporation, and for a proper purpose.

To effectively discharge their duties, directors must take necessary steps to enable them to effectively guide and monitor management of the organisation.[6] Boards need to exercise active stewardship to ensure they have meaningful oversight of their organisation and management. Directors should take a diligent interest in information provided to them and apply an enquiring mind in the discharge of their responsibilities.[7]

The board should ensure processes and practices are implemented so that the organisation operates within the board's strategic goals and stated risk appetite. Officers should give their boards all information they have that is material to the board's decision making.[8] Equally, the board needs to ensure it is receiving adequate information to make informed decisions.

ASIC's encouragement of active stewardship should not be viewed as a suggestion that directors undertake the role of management. This would defeat the purpose of having a separate body to exercise independent oversight. Instead, active stewardship requires directors to ensure they are properly informed so that they can hold management to account regarding the operation of the company. It requires the board to be the guardian of the long-term sustainability of the company. Where management action (or inaction) is inconsistent with this, the board needs to ensure that the company is brought back on course.

How this report fits into Australia's governance landscape

This report aligns with ASIC's regulatory mission to change behaviours to drive good consumer and investor outcomes, and to promote strong and innovative development of the financial system. It is intended to provide observations and insights into the governance practices of large ASX-listed companies, to encourage directors and officers to enhance their oversight of (and in the case of officers, the management of) non-financial risk in discharging their duties.

ASIC's observations and insights contained in this report are intended to sit alongside market guidance, industry-specific requirements and other relevant reports such as:

- the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*[9]
- APRA's Prudential Standards
- the APRA CBA Inquiry Report[10]
- the APRA Information Paper: *Self-assessments of governance, accountability and culture*[11]
- the Financial Services Royal Commission's Final Report.[12]

6 *Daniels v Anderson* (1995) 37 NSWLR 438.

7 *ASIC v Healey* (2011) 278 ALR 618.

8 *ASIC v Vines* (2005) 65 NSWLR 281.

9 **ASX Corporate Governance Principles and Recommendations**.

10 **APRA CBA Inquiry Report**.

11 APRA, ***Information Paper: Self-assessments of governance, accountability and culture***, 22 May 2019.

12 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry: ***Final Report, Volumes 1-3***, 1 February 2019.

Note on terminology

Corporate governance

Corporate governance is a driver of an organisation's performance. The term 'corporate governance' is broad and has many components.

The ASX Corporate Governance Council's definition set out in the ASX's *Corporate Governance Principles and Recommendations* (Fourth Edition)[13], provides a useful basis:

> The framework of rules, relationships, systems and processes within and by which authority is exercised and controlled within corporations. It encompasses the mechanisms by which companies and those in control are held to account.[14]

Considering the Taskforce's review in the context of Bob Tricker's model of corporate governance[15], the review focused on the monitoring, supervision and accountability aspects of corporate governance.

The Taskforce's review that underpins this report was not a whole-of-company corporate governance review. Rather, it focused on identifying corporate governance practices that impacted director and officer oversight, through the lens of non-financial risk.

Non-financial risk

We adopted a definition of non-financial risk that aligns with the definition that APRA used during its prudential inquiry into CBA[16] (which stemmed from the Basel Committee on Banking Supervision and ASIC's market supervision guidance).

We adapted APRA's definition to cover more than just prudential institutions, so that 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[17]
- **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[18]
- **conduct risk** – the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees.[19]

These risks, although called non-financial, may lead to very significant financial loss if they are not well managed.

During our review, we focused on compliance risk as the primary risk through which director and officer oversight of non-financial risk was observed. Throughout the report we specify where findings relate specifically to compliance risk, and where they relate to non-financial risk more broadly.

13 **ASX Corporate Governance Principles and Recommendations.**

14 Taken from Justice Owen's report of the Royal Commission into HIH Insurance, *The Failure of HIH Insurance Volume 1: A Corporate Collapse and Its Lessons, Commonwealth of Australia*, April 2003, at page xxxiv.

15 Bob Tricker, *Corporate Governance Principles, Policies, and Practices* (Second Edition), Oxford University Press, 2012.

16 **APRA CBA Inquiry Report**.

17 **APRA CBA Inquiry Report**, page 7; Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011.

18 **APRA CBA Inquiry Report**, page 7; Basel Committee on Banking Supervision, *Compliance and the compliance function in banks*, April 2005.

19 **APRA CBA Inquiry Report**, page 7; Australian Securities and Investments Commission, *Market Supervision Update Issue 57 – Conduct Risk*, March 2015.

Companies that participated in the review

The Taskforce reviewed governance practices relating to director and officer oversight of non-financial risk in the following companies:

- AMP Limited
- Australia and New Zealand Banking Group Limited
- Commonwealth Bank of Australia
- Insurance Australia Group Limited
- IOOF Holdings Limited
- National Australia Bank Limited
- Westpac Banking Corporation.

All companies within the scope of the review produced documents under notice and participated in voluntary interviews with ASIC.

This report was produced to give the broader market insights into corporate governance practices generally. For this reason, while we have named the companies that participated in this review, the report does not publicly attribute governance practices to individual companies.[20] Before publishing this report, we gave these companies individual feedback letters detailing our findings and observations. This feedback aims to drive improvements at an organisational level.

Methodology

The Taskforce used a multi-disciplinary approach to its governance review. Findings and observations set out in this report are based on a review of documents received under notice, as well as other public and non-public documents, and information gathered from interviews with directors and officers.

See Appendix 2 for more details about the methodology used and information relied upon to inform ASIC's review.

Participation

A large part of this work depended on voluntary participation in the ASIC-led interviews as well as voluntary participation in the behavioural analysis conducted by an external expert. The time commitment was significant and we appreciate these organisations making themselves available.

Companies that opened their doors to ASIC showed willingness to have their governance practices observed and to receive ASIC's feedback on areas for improvement. This shows board-level acceptance that there are still things to be done. More importantly, it also shows willingness to act on feedback about improvements that could benefit the organisation and its shareholders.

20 To ensure individual governance practices are not inadvertently identified, companies receive a random identifying letter in each graphic or dataset, i.e. Company A in one chart is not the same company as Company A in the next chart.

Risk appetite statements

How do directors and officers use risk appetite statements to oversee non-financial risk in their companies?

Boards are often cited as having two fundamental functions – to set an organisation's strategy and its risk appetite.

An organisation's risk appetite is the amount of risk it is willing to accept in pursuing its strategic objectives. This sets the parameters within which management is expected to operate.

It is good practice for boards of all large listed companies to establish a board-approved risk appetite, in accordance with the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*[21], and metrics for measuring compliance with that appetite. Twelve per cent of ASX 100 companies are subject to APRA regulation and therefore are required to have a board-approved RAS.[22] All companies subject to this review had a board-approved RAS.

Overall, we observed that boards' stated compliance risk appetite did not appear to reflect their actual risk appetite, with companies consistently operating outside their appetite. This was not confined to compliance risk, but was typical of non-financial risks generally, which in some companies we observed to be at levels outside appetite for significant periods of time when compared to financial risk (see page 14). Metrics that were supposed to measure where the company was sitting against its risk appetite did not provide a representative view of the level of risk the company was exposed to. Reporting on non-financial risk did not always align with the metrics in the RAS, reducing boards' visibility of how the company was tracking against its risk appetite.

In general, we also observed that companies' risk appetite and metrics were less mature for non-financial risks than for financial risks, where metrics were more granular and comprehensive.

This chapter contains ASIC's observations about how boards used RASs to oversee and monitor non-financial risk, particularly compliance risk.

21 In the third edition, this appeared in the commentary. In the fourth edition it appears in recommendation 7.2. The fourth edition's effective date is the first full financial year beginning on or after 1 January 2020.

22 See APRA Prudential Standards CPS 220 and SPS 220. APRA-regulated registrable superannuation entities (RSEs) are required to have a board-approved RAS at RSE level.

What role can RASs play in assisting boards to oversee non-financial risk?

Directors of large, complex companies are charged with the substantial role of overseeing risk management. Used properly, a RAS can be an important tool to assist in this task. A sophisticated RAS enables the board to:

- communicate the desired risk tolerance for specific risks to the company
- monitor and measure how the company is operating against its stated appetite for a particular risk
- mobilise resources and strategies to return the company to within appetite where reporting indicates that it is operating outside appetite.

Effective oversight of risk in large, complex companies is a multi-faceted exercise, requiring analysis, input and reporting from a number of sources. The RAS is only one of these sources; however, it can provide the board with critical insight into the status of key risk areas.

To be an effective tool to oversee risk, a RAS must:

- clearly articulate the level of risk the board is willing to accept and its tolerance regarding that risk
- have metrics that are sufficiently representative, to enable the board to measure where the company is operating against risk appetite and tolerance.

There must also be:

- meaningful management reporting to the board on risk appetite metrics
- a board that holds management accountable, when the company operates outside risk appetite.

General features of RASs reviewed

All seven companies had a board-approved RAS, consistent with being subject to APRA regulation. The infographic (below right) sets out the features for compliance risk in each organisation's RAS.

Six of the seven companies set out their compliance risk appetite and included metrics to measure the level of compliance risk they were exposed to. Some companies' RASs included markers to indicate to the board when they were approaching appetite.

For example, one company that sought to measure when it was approaching appetite limits used an 'early warning' level. It also had an 'intervention' level, which indicated when it was outside appetite. An early warning was reported as 'amber' and meant that a 'discussion point' had been reached. An intervention was reported as 'red' and meant that a point had been reached where action was required to return to within appetite. This two-stage process appeared to provide meaningful indicators of the actions the board and management were required to take at the different risk levels.

It was concerning that one company did not include compliance risk appetite in its RAS, stating it was 'not applicable' for the listed entity, and rather relied on the RASs of its subsidiaries to articulate this risk (although it did not appear to adopt this approach for financial risks). This raises a number of issues:

- It suggests that the board had not consciously considered a specific risk appetite for the conduct of that company (even though it had distinct compliance risks as the result of being a listed entity as well as being the parent of various operating subsidiaries).
- The RAS failed to make clear to management what level of compliance risk the board was willing to accept.
- The board's failure to articulate its compliance risk appetite meant there was a lack of board-approved metrics for measuring compliance risk exposure across the organisation.
- The board received reports on what management determined was relevant, rather than reports aligned to metrics and its appetite for compliance risk.
- The board did not have a standard against which to hold itself and management accountable for acceptable levels of risk.

Features of the RAS – compliance risk

6/7 companies articulated a compliance risk appetite

6/7 companies had metrics to measure whether they were inside or outside compliance risk appetite

2/7 companies had metrics which measured whether they were approaching compliance risk appetite

1 Boards need to hold management to account when companies are operating outside appetite

Our review indicated that all too often management operated outside appetite in relation to compliance risk, and non-financial risk more generally, for extended periods.

For several companies, it was the norm – not the exception – to operate outside risk appetite for non-financial risk. This is in stark contrast to the position for financial risk, as illustrated in the following diagrams. They contrast two companies' compliance with their non-financial risk appetites against their financial risk appetites.

Company A – financial risk vs non-financial risk (2017–18)

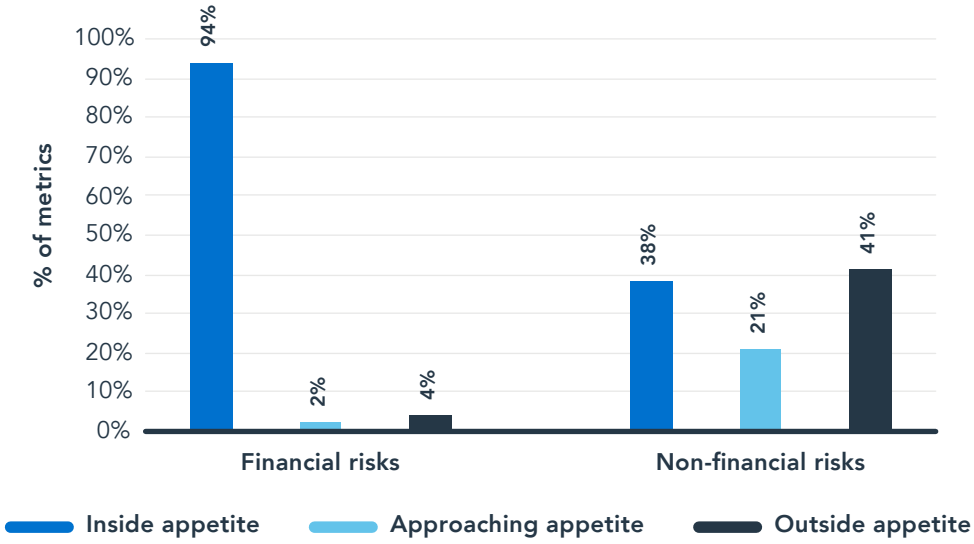
3 OUT OF 3 financial risks sat within appetite
for the whole 24-month period

1 OUT OF 3 non-financial risks were approaching appetite
for the whole 24-month period

2 OUT OF 3 non-financial risks were outside appetite
for the whole 24-month period

The infographic (below left) shows that the company was outside appetite or approaching appetite for non-financial risks for the 24-month period of the review. By contrast, no financial risks were outside appetite or approaching appetite during this period. While the minutes demonstrated instances of the BRC engaging (in varying degrees) with specific compliance issues, there was no clear evidence in the minutes that the BRC actively sought to urgently return the company into appetite for a sustainable period. We observed issues being addressed as they arose, rather than the board stepping back and considering compliance risk exposure holistically and prioritising the resolution of root causes of appetite breaches. The practical implication of this was that operating outside of appetite for non-financial risk was tacitly accepted in this organisation.

Company B – operating outside appetite or approaching appetite – financial risk vs non-financial risk as at September 2018



The chart above shows another company in which 62% of non-financial risk metrics were outside appetite or approaching appetite, while only 6% of financial risk metrics were outside appetite or approaching appetite. In this organisation, one non-financial risk remained outside appetite for 30 consecutive months, while another moved inside and outside appetite over 30 consecutive months. This raises a question about whether the company was addressing the fundamental or root causes of the relevant risk, and suggests tacit acceptance by the board of operating outside of appetite for these non-financial risks.

Better practice

Active stewardship requires the board to hold management to account when a company operates outside the board's stated risk appetite.

The board cannot simply express its disappointment at a risk staying outside appetite for a stated period. It must do more to quickly return the company to within appetite. This includes challenging the actions and timeframes within which management proposes to resolve the issue. Prioritisation and slippage should be monitored and accounted for.

In the absence of tangible and timely plans to return to within appetite, boards should consider whether management needs to cease practices that are causing companies to be outside appetite.

Many companies we interviewed acknowledged they were operating outside appetite for an extensive period, and that it would take some time to return to within appetite. However, one company stated that where it identified it would be outside appetite for a lengthy period, it would change the way it provided certain products and services.

Returning a company to within its risk appetite can be resource-intensive. Several companies noted that the main barrier was finding the right expertise in the market to address the issues. Boards must adapt to their operating environment – where there is a shortage of necessary expertise, they must consider whether current operations should change in light of the heightened risk.

Boards should also require management to undertake root cause analysis, or thematic analysis, to identify underlying causes of recurring breaches of appetite. This is imperative where seemingly distinctive compliance events continue to cause the company to operate outside appetite (or dip in and out of appetite). The board should proactively seek this analysis from management. During our review, we saw sporadic evidence of boards requesting root cause analysis or 'deep dives'; however, this should occur as a matter of course to help deal with recurrent issues.

Where required structural or long-term solutions are being implemented, the board and management should concurrently consider flexible short-term solutions as a priority to ensure they are operating within board-approved appetite during this time. These could include engaging external resources (e.g. professional services firms) or reviewing the stated risk appetite, rather than simply accepting that they will be operating outside appetite for a long period without appropriate mitigants.

Boards need to ask themselves:

> **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?**

If the answer to either question is 'no', the board is likely to be seen to be tacitly accepting a higher risk appetite for its company and should consider its own accountability. This tacit acceptance in stark contrast to the company's stated risk appetite may undermine trust and credibility in the company's commitment to governance in this area.

2 The full board must engage with the RAS for it to be an effective oversight tool

Setting risk appetite is a fundamental board function. Therefore, it requires full board engagement.

We saw that in one organisation, the BRC, with only a subset of non-executive directors, approved the RAS, instead of the full board approving it at a board meeting. If only a subset of directors formally approves a RAS, it affects the ability of all directors to engage with the details in the RAS and oversee risk management.[23]

Our review also identified board members in two companies who couldn't explain the metrics accompanying the compliance risk appetite in the RAS, or who had an inconsistent understanding of some metrics, having not engaged with the details in the RAS.

Better practice

A Financial Stability Board report[24] found that when a board approves a RAS – rather than simply 'receiving' or 'noting' it – board members have a greater understanding of the risk appetite. It follows that boards that *actively* engage in the approval process – rather than treating it as a box-ticking exercise – have a greater understanding of their risk appetite. The board and BRC minutes of three companies reflected some level of active engagement with the content of the RAS.

The level of board engagement with the RAS also sends a strong message to management that the board considers the RAS to be important. Lack of engagement diminishes the likelihood of effectively using the RAS to oversee risk. Boards using a RAS as a key oversight tool must ensure that it is up to date and dynamic, and reflects their appetite.

Directors should ask themselves:

> **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?**

Directors should also ask themselves a similar question in relation to all non-financial risks covered by their RAS.

23 See **Attachment A** at page 7 for discussion regarding non-executive directors' understanding of operational issues in the business

24 Financial Stability Board, ***Principles for an Effective Risk Appetite Framework***, 2013.

3 Risk appetite needs to be clearly expressed, reflecting actual appetite

A RAS must clearly express the board's appetite for the level of risk it is willing for the company to accept.

The RASs we reviewed articulated the compliance risk appetite in a variety of ways. The following infographic maps out those approaches.

How did companies articulate their compliance risk appetite?

2 COMPANIES

Statement that 'we comply with all laws' or 'full regulatory compliance is required'

1 COMPANY

Statement that they maintain an extremely limited and reducing tolerance to breaches

2 COMPANIES

Statement that they had no appetite for intentional, deliberate or negligent non-compliance

1 COMPANY

No statement of appetite expressed

1 COMPANY

Statement that they had no appetite for deliberate, material or notable systemic breaches

The risk appetites of several companies did not appear to match their actual tolerance levels. This was shown by these companies consistently operating outside their boards' stated risk appetite (see pages 14 and 15).

Some of these companies' RASs made statements of full regulatory compliance. While adopting these types of aspirational statements sends a message to staff, doing so without reinforcing them through strong accountability and consequences significantly undermines the effect of the statement.

Where the company is aware that the statement bears no resemblance to its actual risk position – either because it has operated outside appetite for some time or knows it has never achieved that level of compliance – it can confuse or even mislead employees and third parties, including regulators, that receive the RAS.

Better practice

In our discussions, many companies acknowledged the challenges of articulating their compliance risk appetite. But few expressed an urgent need to clarify their appetite.

We think boards can do more to express their appetite in a way that is meaningful and aligns with their actual appetite. Compliance with legal and regulatory obligations must be a high priority for boards.

Another useful aspect of many of the compliance risk appetite statements we observed was the addition of statements describing the companies' expectations when non-compliance did occur – for example, the expected process for identifying, escalating and remediating breaches.

Boards should ask themselves:

> **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?**

4 Metrics should be a proxy for the actual risk position to enable meaningful monitoring of appetite

The RASs we saw used a variety of metrics to help the company monitor compliance risk.

The metrics we observed for compliance risk often measured discrete issues or areas of compliance, rather than providing insight into the broader compliance behaviour of the organisation. This seems problematic, given that most risk appetites were described in terms of the broader compliance of the organisation.

Many companies' metrics focused on breaches of specific laws or regulations to measure compliance risk. However, relying on such metrics focuses on lagging indicators of compliance, rather than leading indicators of compliance risk exposure. See page 22 for more information on using leading and lagging indicators.

In some instances, the reliability of certain metrics was also in debate. For example, one entity had a metric for compliance risk that measured compliance with internal controls. The Chief Risk Officer (CRO) questioned the accuracy of the metric and suggested it was going to be abandoned. In contrast, when separately questioned about the metric, the BRC Chair stood by its effectiveness and suggested no plans were in place to abandon it.

Better practice

Boards need to select and develop metrics that are representative of the risk they are measuring. Increasing the number of metrics does not necessarily provide the solution, though boards need to consider whether their metrics are sufficiently representative to 'cover the field'.

Boards should ask themselves:

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

5 Metrics for measuring risk exposure should align with the stated risk appetite

A number of companies set their compliance risk appetite with reference to how breaches occurred – for example, they expressed zero tolerance for breaches that were deliberate, intentional or negligent. However, the metrics adopted to measure compliance risk largely did not measure how breaches occurred, focusing instead on the nature of breaches.

One company that stated it had no appetite for 'deliberate, material or notable systemic breaches' had a metric to identify material breaches that had occurred, but no metrics to determine whether there were any deliberate or notable systemic breaches. The inability to monitor whether breaches are a result of systemic issues significantly limits effective oversight.

It is also unclear whether a causal appetite rather than an outcome-focused appetite correctly articulates the desired outcome of a well-designed and well-executed risk management framework.

Better practice

Well-developed compliance risk metrics should enable a company to measure how it is complying with its appetite. If a company is measuring its compliance risk appetite by referring to how breaches occurred, it should try and measure that. And the board should still require metrics that facilitate insights into the organisation's overall level of compliance (see page 20), by providing a representative picture of risk exposure.

Similarly, boards should also be able to access information to identify systemic issues and perform root cause analysis.

Boards should ask themselves:

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

6 Metrics should include leading and lagging indicators

Most of the metrics we observed were lagging indicators, measuring breaches of the law that had already occurred.

We saw evidence of some companies attempting to use leading indicators to create early warning systems or identify rising risk levels within the business. For example, we observed leading indicators measuring the number of reopened internal audit issues, or breaches of internal policies as a precursor to breaches of the law. However, these were not as prevalent as lagging indicators.

While using leading indicators in metrics is better than just measuring actual regulatory breaches, the measures being adopted appeared to need further development before they could comprehensively identify when an entity was approaching its risk tolerance limit. Well-developed leading indicators also provide a representative picture of rising risk levels (see page 20).

Better practice

Boards should aim to include leading indicators in metrics that raise an early warning for rising risk levels. This would enable boards to require management to act early to avoid breaching a particular tolerance.

Using leading indicators is a well-developed practice for measuring safety risk outside the financial services sector, where the focus has shifted from actual incidents to 'near misses'. There appears to be more scope for using leading indicators in relation to other non-financial risks such as compliance risk.

Boards should ask themselves:

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

7 Boards should consider if metrics for a non-financial risk is comparable to those for other risks

Overall, our review indicated that metrics for financial risk were usually more specific, granular and quantitative, compared to non-financial risk metrics. Financial risk metrics were generally more consistent across the companies reviewed (with particular consistency across the banking institutions), whereas non-financial risk metrics varied much more significantly across the sample.

In one company we observed, metrics for one financial risk were broken down into portfolios, industries and jurisdictions, with each group having a number of quantitative metrics that included a trigger level and a limit. By contrast, compliance risk had just three metrics: the number of new, significant and reportable breaches of law; the number of breaches of specific policies; and one internal compliance measure. Only two metrics had both a trigger and a limit (the third had only a limit).

Another company used 88 metrics to measure financial risks and 14 metrics to measure non-financial risks. While having more metrics does not necessarily translate to better monitoring, this company measured financial risk by jurisdiction, product type and subsidiary owner. By contrast, non-financial risks were commonly only measured according to group-wide total occurrence.

Better practice

Boards need to consider the impact that metrics have on the depth of analysis for non-financial risks. Metrics should provide insight into broader compliance behaviour. Boards should recognise that 'what gets measured gets managed'.

Boards should reflect on how their metrics for compliance risks and other non-financial risks compare to metrics used to measure more mature non-financial risks such as workplace health and safety in mining and construction companies.

Boards should ask themselves:

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

Metrics should provide insight into broader compliance behaviours. Boards should recognise that 'what gets measured gets managed'.

8 Reporting to the board should be aligned with risk appetite and metrics

Management reporting to the board about where the company sits in relation to risk appetite is only one aspect of risk reporting, but it is an important one. It determines the usefulness of the RAS as a risk oversight tool.

If management does not report to the board against the metrics in the RAS, the board cannot tell whether the company is operating inside or outside its risk appetite.

Of the six companies we observed that included compliance risk metrics in their RASs, one company's CRO report did not align compliance risk reporting with the metrics in the RAS. Rather, it reported against other metrics or measurements, creating a disconnect between the RAS and risk reporting. This disconnect may have occurred due to shortcomings of the relevant RAS metrics. In another company, non-financial risk metrics were not reported in the headline CRO report, but instead in the Compliance Officer's report. In contrast, financial risk metrics were included in the headline CRO report (see page 29 for more information on the need for reporting to give adequate prominence to material non-financial risks).

In other companies, management risk reporting better aligned with the metrics in the RASs, including reporting to the board against the company's stated appetite. The degree to which this alignment translated into effective reporting depended on those metrics being meaningful.

Better practice

Management should report to the board with meaningful data that shows how the company is operating compared to its risk appetite. By aligning its reporting, it provides a clear view of the level of risk the company is accepting, compared to what the board is comfortable with.

One organisation's compliance reports were particularly useful in that they showed how it was operating against its compliance risk appetite, including risk mapping that identified deteriorating trends in certain compliance categories that could increase the compliance risk. This gave the BRC advance warning of potential increases in compliance risk levels.

Risk reporting at the management committee level that is aligned to the RAS can also help the board's oversight function. It can do this by engaging management on the board's appetite for non-financial risk, and enhancing the quality of management reporting to the board.

We saw some evidence of this in one company. This could be further enhanced by ensuring that management has data on who is responsible and what needs to be done to return the company to appetite, enabling it to feed this information to the board.

Board members should ask themselves:

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

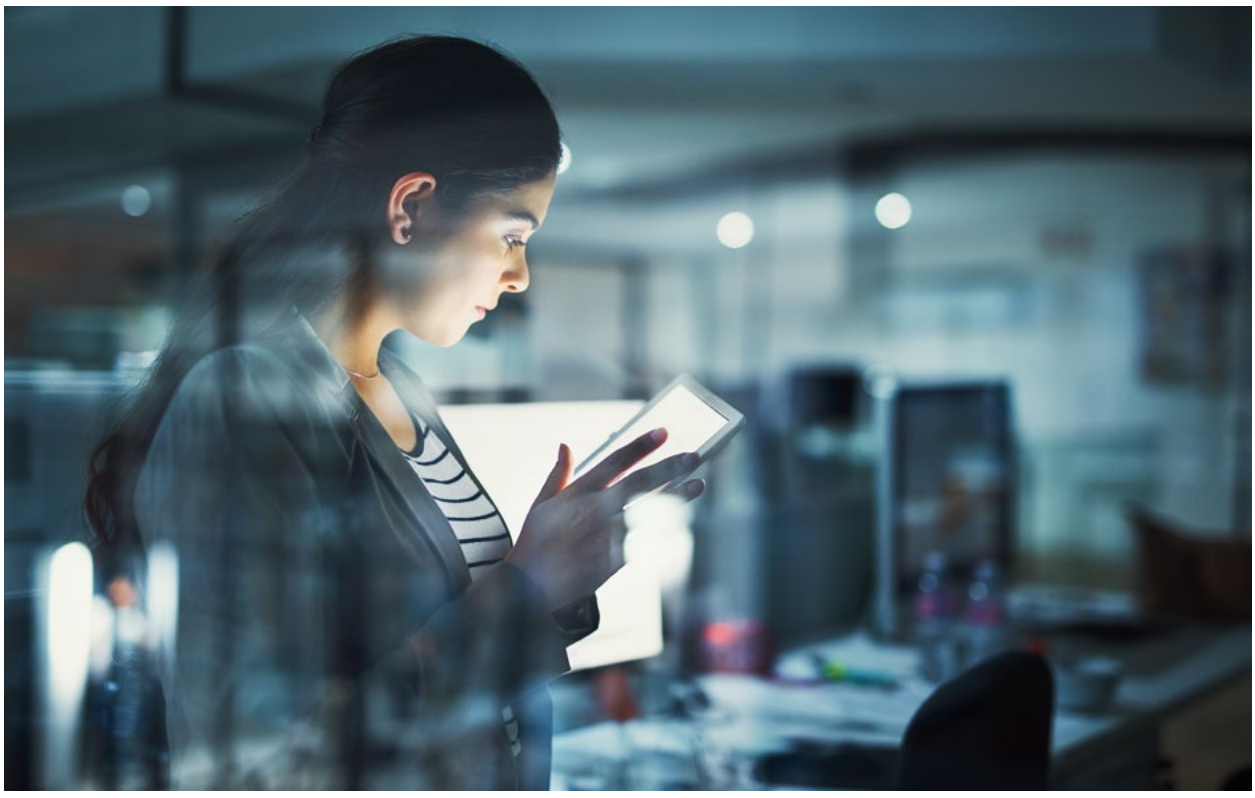
International trends

Companies around the globe face similar challenges in expressing measurable appetites and metrics for non-financial risks, and aligning business and risk reporting. International trends show that efforts are being made to overcome these challenges and use risk appetite as a proactive risk management tool.

Internationally, we have observed differing practices regarding the structure of operational and compliance risk functions in businesses. While some companies in the United Kingdom have brought their operational and compliance risk functions together, some in Europe have separated them. The European Banking Authority's (EBA's) governance guidelines[25] encourage ensuring appropriate authority and stature to the heads of internal risk and compliance functions. For some large and complex institutions, this is occurring through separating risk and compliance.

Companies are also adopting more forward-looking indicators and automated data aggregation to move towards real-time dashboard reporting that shows risk compared to appetite. They are also using data mining and analytics to help identify trends and undertake root cause analysis.

Some companies are also seeking to be explicit about who is accountable for each type of non-financial risk, increasing the accountability of the business (as opposed to risk and compliance functions) for compliance risk. For example, in the United Kingdom, the Senior Managers and Certification Regime, which is similar to the Banking Executive Accountability Regime, has increased the focus on responsibilities and accountabilities. This is driving boards to proactively manage risk exposures.



25 EBA Guidelines on Internal Governance, EBA/GL/2017/11.

Information flows

Are boards getting the right information to enable them to oversee and monitor non-financial risk management?

Effective oversight is informed oversight. Directors need sufficient information to hold management to account and discharge their stewardship over the company's assets.

This does not require that every piece of information be provided to directors. To adequately oversee and monitor non-financial risk, boards need management to provide timely and accurate information that focuses on material non-financial risks. Where the information lacks these qualities, poor oversight, accountability and decision making are inevitable.

Responsibility for the quality and nature of reporting to directors should not solely lie at the feet of management or the company secretary. Directors need to actively engage with this process. They should ensure their organisation has systems and processes to get them the *right* information needed to perform their oversight and monitoring functions.

This section contains ASIC's observations on information flows:

- from management to the board
- between board members
- through committees.

Our review considered verbal and written communication, focusing on whether boards are getting the right information to enable informed decision making on non-financial risks.

Overall, we observed that:

- material non-financial risk information was often buried in dense, voluminous board packs
- it was difficult to identify the materiality of key non-financial risks in information being presented to the board
- undocumented board sessions and informal meetings between directors had the potential to create asymmetric information at board level, if not well managed
- board committees needed to do more to ensure that information flows to other committees and to the full board were formalised and conveyed key risk issues to all board members.

1 Material information should not be buried in lengthy board packs or reports

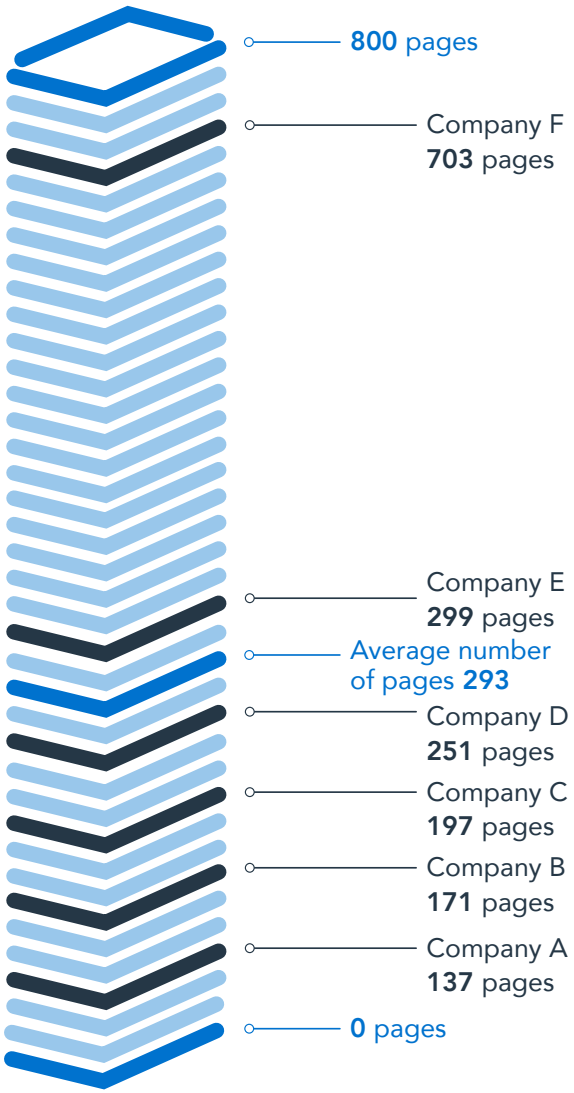
Directors need to have sufficient information to understand the nature and likely impact of material issues facing the company. However, our review indicated that board packs were so dense and voluminous that it was unclear whether their primary purpose was to:

a. inform directors in the most effective manner, or

b. absolve reporters from exercising judgment as to what information should be omitted.

Papers presented to the BRC are a key part of the information flow on non-financial risks from management to the board. The infographic (right) sets out the average number of pages for BRC packs reviewed. It shows that packs presented to BRC meetings averaged just under 300 pages, with one organisation's papers averaging just over 700 pages.

Average number of pages in a BRC pack



The volume of papers that directors are required to read needs to be considered in the context of the growing trend for directors to attend more committee meetings and the common practice to hold committee meetings and full board meetings on consecutive days.

One Chair, who had been working to reduce the size of board packs, commented that directors had recently received packs for all committees – including the BRC and full board meetings – which totalled 900 pages. Reflecting on this, it was the Chair's view that the issues could be explained in 130 pages. The length of board papers often far exceeded an organisation's own guidance and template length.

Better practice

It is not length itself that is the issue – rather, it is *unnecessary* length. When directors themselves consider that the information they need could be explained in less than 25% of the volume provided, work needs to be done to ensure concise management reporting that focuses on the key non-financial risks. Directors need to be proactive in requiring management to deliver information in a form that will help them to fulfil their oversight and monitoring mandate.

We do not believe that imposing and enforcing a maximum page limit will solve this issue. But the fact that organisation-specific guidelines are not being enforced suggests that chairs have not been sufficiently engaging with the nature of reporting provided to them.

Boards should ask themselves:

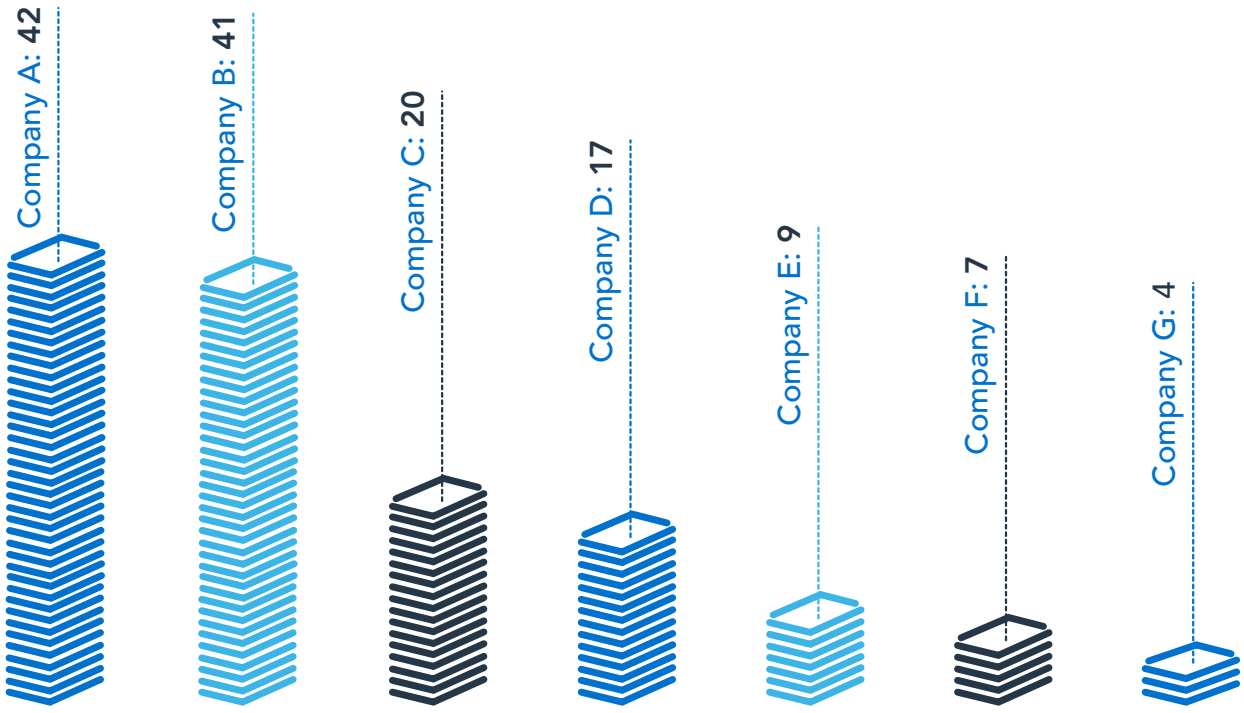
> **Is the breadth and materiality of information that management provides correctly calibrated to help us perform our oversight function?**
>
> **Is the information we receive on non-financial risk of a similar quality to that we receive on financial risk?**

2 Management reporting should have a clear hierarchy for non-financial risks that prioritises their importance

Directors commented that the information in board packs was dense, making it difficult for non-executive directors to understand its relative impact and importance. Many directors said talking to relevant members of management at a meeting (or in free-flowing discussions outside a meeting) provided useful context. This suggests that information in the papers is inadequate, and that context is needed to accompany the papers.[26]

CRO and compliance reports – which are key vehicles for informing the board of material non-financial risks – often did not provide a hierarchy showing the comparative importance of key non-financial risks. CRO reports varied in length and depth of information, and there is scope to more effectively prioritise information. The following infographic shows the average page length of 'headline' CRO reports – that is, CRO reports that were designed to highlight key risks, 'cover the field' or summarise other risk reports.[27]

Average page length of 'headline' CRO reports



26 See **Attachment A** at page 7 for discussion regarding roadblocks to understanding and verifying information provided by management.

27 Based on a review of reports from the second half of 2018. One organisation only recently introduced CRO reports in this format so its average is based on one report.

One CRO report contained static headings for specific risks and mainly detailed green-rated risks first. This has the effect of starting with 'good news', while risks that were over the tolerance limit or at a trigger threshold were reported later.

Other CRO or compliance reports placed key non-financial risk information in appendices to the reports. We observed some reports that cross-referenced other reports or BRC agenda items, but often the links between multiple reports were unclear or not mapped. This creates scope for information overlaps and gaps, and can make it difficult to determine the materiality of an issue across an organisation. Where this occurs, the board has to interpret the possible organisation-wide impact of information presented across numerous documents.

Better practice

Boards should not have to search through substantial amounts of information to seek out references to material risks. Management should be required to tell them where to look.

An example of better practice was a compliance report that provided detailed commentary on specific risks, in order of greatest to least severe. The Chair of this BRC noted that this prioritisation was a result of conscious board efforts. Historically, reports contained key information, but it was buried and wasn't being drawn out for the board.

Boards may wish to consider initiatives to improve mapping and synthesis of risk and compliance reports, to ensure they prioritise key non-financial risks. With boards receiving on average 10 to 43 separate papers for each BRC meeting, it is important that they can identify material non-financial risks when reading the reports all together. Summary reports that highlight material issues raised in lengthier reports may also assist the board to prioritise risks.

Boards should ask themselves:

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

3 Material information should not be lost in undocumented closed sessions

The majority of organisations had 'closed sessions' during their BRC meetings, which typically included only non-executive directors, and no management or only the CRO.

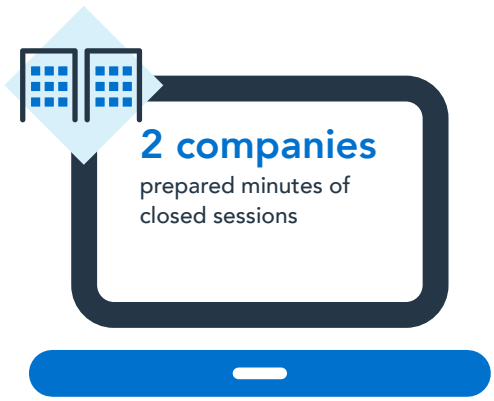
There was strong consensus from directors regarding the significant value of these sessions. They allow non-executive directors on boards or committees to question management without managers present, and to discuss highly sensitive information.

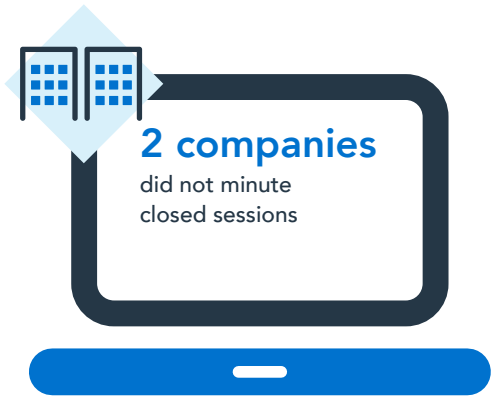
However, when these conversations are not recorded in a way that captures the material issues and action items discussed, it can lead to reduced or impaired information flows to the wider board or management who must address the issues raised.

The BRC at six out of seven organisations had closed sessions in 2018. Despite their importance, two-thirds of the six organisations:

- did not record items discussed or actions arising in minutes
- only minuted certain closed sessions, or only certain parts of them.

Minuting of BRC closed sessions – 2018





Where closed sessions were minuted, the minutes did not convey whether material items were discussed, or whether any action items arose.

This meant that board members who were not present had to rely on verbal updates. More concerningly, there was no detailed corporate record of the matters discussed.

Better practice

Material non-financial risks – indeed, all material issues – and action items arising from closed sessions should be recorded to ensure information flows are not reduced or impaired.

Boards should ask themselves:

> **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?**

4 Minutes should include key discussion points and reasons for decisions

While it is a legal requirement to record minutes of board and board committee meetings, appropriately detailed minutes are also important for ensuring effective information flows around the board, and from the board to management. In addition, minutes can help boards to demonstrate they have exercised active stewardship and performed their oversight and monitoring functions.

The minutes we reviewed were often brief and formulaic. Generally, they lacked sufficient information about topics discussed or key factors in decision making. For example, as set out on pages 31–32, none of the six entities minuted BRC closed sessions with appropriate detail.

While we observed better minute-taking practices over the 2018 calendar year, standards could be further improved. For example, we were generally unable to determine the quality of active oversight by board members due to the limited information in minutes (see page 49 for more information on active oversight at one BRC).

Better practice

The Australian Institute of Company Directors and the Governance Institute of Australia have released a joint statement on board minutes[28], setting out key principles for what matters should be recorded. The statement notes that minutes do not have to be a transcript of board meetings; however, they must record the proceedings and resolutions of board meetings (including board committee meetings).[29] Importantly, the joint statement advises organisations to include the key discussion points and reasons for decisions to help demonstrate that directors have discharged their obligations.

In addition, the joint statement notes that while the level of detail to be captured is a judgement call, it is appropriate for minutes to record 'significant issues raised with management by directors' as well as action items arising.[30] Recording significant issues raised with management and the actions sought from management will help the board demonstrate where they have exercised genuine oversight (see page 48).

Boards should review this joint statement against their own minute-taking practices, including for closed sessions, to ask themselves:

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

28 Australian Institute of Company Directors and the Governance Institute of Australia, ***Joint statement on board minutes – August 2019***.

29 Section 251A, Corporations Act.

30 Australian Institute of Company Directors and the Governance Institute of Australia, **Joint statement on board minutes – August 2019**, page 2.

5 Informal meetings should be conducted in a manner that avoids asymmetric information between board members

Boards receive information from a variety of sources outside formal board meetings and board committee meetings. Many directors commented on the value of discussions at board dinners or during one-on-one or small group meetings before formal board meetings, and insights gained from site visits.

Better practice

We recognise that boards need to interact in a manner that increases their effectiveness, which includes informal meetings. These meetings are a good forum to gain greater understanding of issues and insights into company operations. Boards need to be mindful however of the risks involved where informal conversations result in decisions or actions being agreed upon absent formal frameworks or without the benefit of the entire board's views being considered. Boards should implement practices that minimise these risks, such as monitoring the subject of discussions that are not repeated at a formal meeting, and formally recording key decisions and action items.

Boards should ask themselves:

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

6 Board committees should ensure the full board is updated on material non-financial risks in a timely way

We observed that information flowed from the BRC to the full board or other committees in a variety of ways. The table on the next page depicts the combination of methods different organisations used to update the board on BRC matters, including direct reporting from management, minutes and updates provided by the BRC chair.

As the table on the next page shows, organisations used a variety of methods to update the board. The methods often complement each other. For example, while minutes often weren't available to the board for some months, verbal updates at the next meeting (often the next day) helped fill the gap.

However, most methods also had limitations. For example, minutes were brief (we observed that board minutes were often even briefer than BRC minutes) and verbal updates were often allocated only very limited time on the agenda. While verbal updates have some inherent benefits, relying too heavily on verbal updates without any accompanying analysis reduces objective data-driven reporting; therefore, it increases the risk that the presenter will frame the materiality of risks according to their own understanding or bias.

	CRO attended most or all board meetings	Written CRO/risk report provided at some or all board meetings	BRC minutes provided to board meeting	Verbal update from BRC chair (where not all directors attended BRC)
Organisations with full board membership at BRC				
Company A	✓	Limited[31]		✓
Company B	✓	Limited	✓	
Organisations with all non-executive directors invited to attend BRC (but not all are members)				
Company C	Some	Limited	✓	✓
Company D	✓	Limited		✓
Company E	✓	✓	✓	
Company F	Some		✓	
Sub-set of the board are members and attendees at BRC				
Company G	✓	✓	✓	✓

Organisations that invited all non-executive directors to attend BRC meetings often appeared to provide less detailed reporting to the full board, assuming that all board members would attend the BRC meetings. This becomes problematic when not all directors attend BRC meetings.

As we note in the section on BRCs on page 51, there was an emerging trend toward inviting all directors to BRC meetings, but most companies had not formalised BRC membership for all directors. Therefore, it is possible that the practice of the full board attending in some organisations may subside or reverse. Among organisations that currently invited all non-executive directors to BRC meetings, not all directors attended every meeting.

Better practice

Where not all directors attend BRC meetings, it would be better practice for the CRO to attend the relevant part of board meetings and present a written CRO or risk report. This will help to ensure directors are aware of material non-financial risks discussed during BRC meetings.

The methods that management and the BRC use to update the full board should work together to inform non-attending directors of material non-financial risks discussed at BRC meetings.

Boards should ask themselves:

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

31 Limited – only some CRO reports were provided to the board meeting (i.e. a report on regulatory breaches, or on certain risks).

7 Cross-committee information flow should be formalised

APRA's inquiry into CBA noted that simply having cross-committee membership was not enough to ensure efficient information flows between board committees.[32] This is particularly relevant for large, complex organisations where numerous issues are likely to arise within those forums, and they need to be formally referred across committees to achieve a whole-of-company perspective.

Despite this, some organisations still appeared to rely on cross-committee membership as a key part of their information flows.

Better practice

The Chair of one organisation implemented a 'handover note' system between committees, which was recorded in committee minutes. This was intended to ensure that important issues did not slip through the cracks as a result of relying on cross-committee memberships. The Chair also noted that this process was very effective for signalling to management the importance of specific issues.

The BRC charter of one organisation mandated sharing information with the Board Audit Committee and other board committees where relevant, while another required that relevant chairs hold meetings, where necessary. Formalising information sharing in this manner may help to introduce more reliable information flows between committees.

Boards should ask themselves:

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

32 **APRA CBA Inquiry Report**.

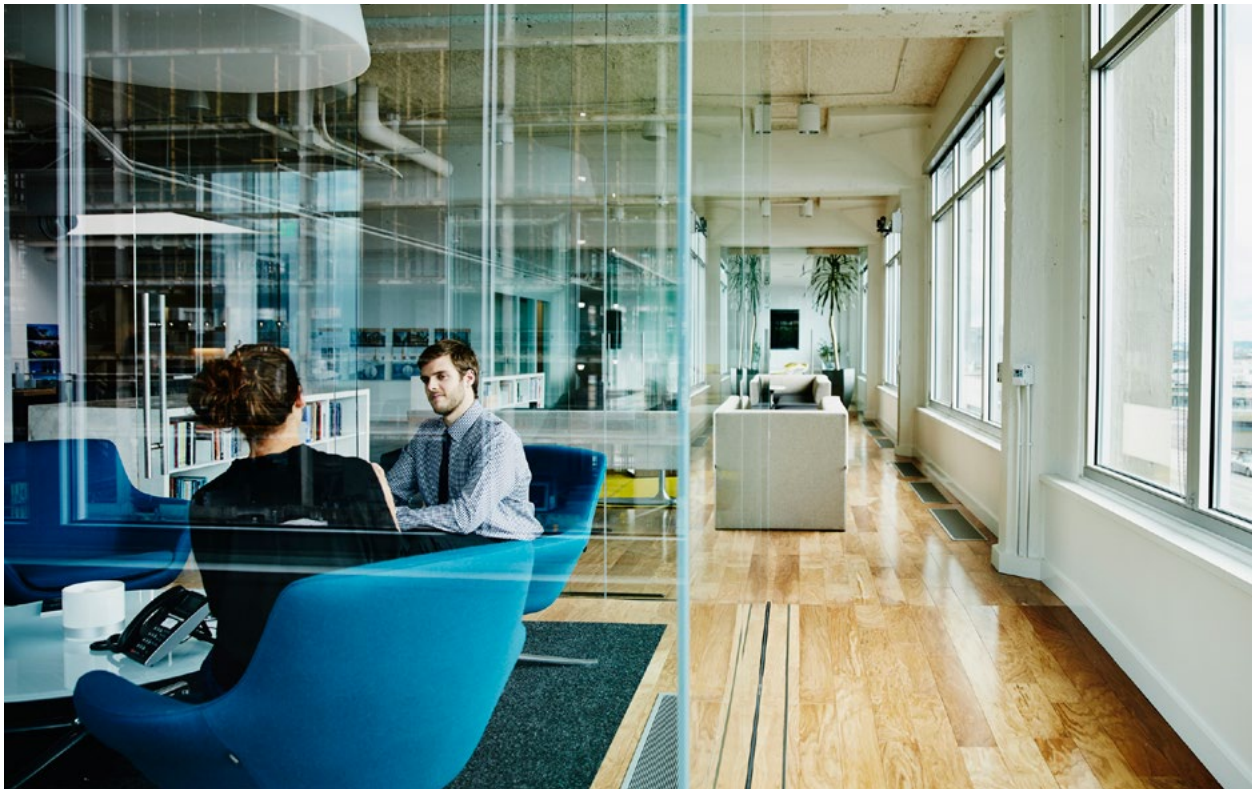
8 Boards should explore alternative solutions to enhance information flows

Designing and implementing a system that effectively identifies and escalates issues to the board is clearly complex. All organisations we reviewed were grappling with this challenge – and clearly there is no 'silver bullet' solution.

Given the importance of this issue, we encourage organisations to think laterally about how they can improve information flows. In many cases, this may involve enhancing and refining existing processes. While we are not encouraging organisations to introduce new structures or frameworks for the sake of having additional processes, those that address a root cause of the problem can have a positive impact.

We reviewed one organisation's executive-level non-financial risk committee to determine how it affected information flows to the board. While having management committees that focus on non-financial risk can have benefits, boards need to:

- consider their motivation for establishing such a committee (that is, is it a 'form over substance' solution to address poor information flows?)
- consider whether existing structures can deliver the desired outcomes
- ensure that such a committee delivers on the board's desired goals.



Case study: Executive-level non-financial risk committee

Review

We reviewed the manner in which one executive-level non-financial risk committee helped the board oversee non-financial risks, including through identifying and escalating risks. We considered how the committee shaped information received at the board level, and in turn aided board oversight of non-financial risk.

Key observations

We observed the following:

- The committee appeared to enable informed updates to the board on non-financial risks. It shaped agendas and items for BRC and board meetings, to ensure key issues were addressed.
- Its existence heightened awareness of the materiality of risks, and provided opportunities for management to cascade messages downstream and increase awareness of issues affecting the organisation more widely.
- Business unit updates at committee meetings were largely verbal. This supported free-flowing discussion and reflection on how issues affected other business units. (However, see page 35 for the limitations of verbal updates.) Nevertheless, we observed limited consideration of systemic issues or root causes of issues that may have been valuable to the board.

We also observed the following examples of better practice for the executive-level committee:

- Its reporting was aligned to the company's RAS, which helped management provide the board with meaningful reporting on risk appetite.
- The committee appeared to enable more coordinated thinking around non-financial risks, enabling management to 'join the dots'. The Chair of the full board said it had helped highlight materiality and context of non-financial risks for the board.

International trends

The themes we observed in our review were also evident internationally, with entities facing challenges including:

- unfocused and voluminous reporting
- a wide variety of reports on granular risk types, and insufficient streamlining of reporting on non-financial issues.

There is also greater focus on automating non-financial risk reporting, including the use of faster and integrated data aggregation capabilities to enable efficient and timely escalation of issues. Technology and data solutions that achieve this are often referred to as 'regtech' or 'corptech'.

According to a recent Bank of England (BoE) report, 57% of regulated firms that responded to a survey said they were using artificial intelligence applications in their risk management and compliance areas.[33] BoE noted the benefits of such applications but warned of their limitations – human incentives still impacted the quality of the systems, and the transition process was resource-intensive and presented unique risks. These include the need for new skill sets at board and management level.[34] Applications may also unintentionally obscure the root causes of issues, with users being unable to determine whether they need to resolve a systems issue or an organisational issue.[35]

Other corporate governance experts have also warned that new technologies will not solve all corporate governance issues.[36] Accordingly, while technology and data solutions can be useful in assisting organisations to navigate complex problems with issue identification, escalation and information flows, they should not be solely relied upon to solve such issues. Directors also need to be aware of the risks, as with any new technologies.

In another global trend, management-level non-financial risk committees have become increasingly common.[37] One international bank has one or two board members attend management-level non-financial risk committee meetings as a challenge point, and to ensure that the board is aware of emerging issues early.

33 ***Managing Machines: the governance of artificial intelligence***; speech by James Proudman, Executive Director of UK Deposit Takers Supervision. FCA Conference on Governance in Banking, 4 June 2019.

34 As above.

35 As above.

36 Enriques, L., ***Corporate Technologies and the Tech Nirvana Fallacy***, European Corporate Governance Institute – Law Working Paper No. 457/2019.

37 **APRA CBA Inquiry Report;** Deutsche Bank in Germany has established a non-financial risk committee at its management board level. Dutch bank ING Group has created a similar committee. To address specific non-financial risks, American organisation Johnson & Johnson has established a management-level triage committee, and US pharmaceutical company Pfizer has a board-level regulatory compliance committee to oversee certain compliance risks.

Board risk committees

How do directors and officers use board risk committees – in practice – to oversee non-financial risk in their companies?

Why have a BRC?

BRCs can play a vital role in:

- bringing independent judgement to risks
- focusing the board's oversight of non-financial risks
- reviewing and debating risk frameworks and appetites
- monitoring compliance with risk tolerances
- monitoring material risks (including emerging risks) through the escalation of significant incidents and breaches
- identifying root causes and trends.

Our review indicated that companies were generally seeking to use BRCs to achieve the above outcomes, but they could be more effective in doing so. This chapter sets out some areas for improvement in governance practices.

The use of BRCs

The ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* encourages all listed companies to have a committee that oversees risk.[38]

As the infographic below demonstrates, 87 of the ASX 100 companies have a board committee that includes risk in its mandate. These committees are a mixture of either standalone risk committees or combined committees (with the most common combination being an audit and risk committee). Of the 24 companies with a dedicated BRC, 12 are required to have a BRC under APRA's Prudential Standards.[39]

ASX 100 companies and BRCs

38 **ASX Corporate Governance Principles and Recommendations.**

39 This data is accurate as at 1 September 2019.

Each of the companies we reviewed had a standalone BRC.

Having a standalone risk committee appears to be increasing in prominence internationally – the Organisation for Economic Co-operation and Development's (OECD's) *Corporate Governance Factbook 2019* reports that around one-third of jurisdictions require or recommend that companies have a separate risk committee – this is double the number reported in the 2015 edition of the OECD *Corporate Governance Factbook*.[40]

ASIC encourages all large listed companies to consider whether creating a dedicated BRC would benefit their long-term interests given:

- the broad mandate and workloads of audit committees
- the ability of risk committees to focus on non-financial and financial risks
- the inherently backward-looking nature of the work of audit committees, compared with the forward-looking nature of risk committees
- the degree to which dedicated risk committees can enhance the focus on risk within companies.

Regardless of whether companies have a standalone or combined risk committee, ASIC encourages all boards that have committees with risk in their mandate to consider revising their practices in light of the observations in this chapter.

40 ***OECD Corporate Governance Factbook 2019***, 11 June 2019, page 124.

1 BRCs need to dedicate enough time to discharging their mandate

BRCs have broad mandates. The charters reviewed set out duties ranging from considering risk frameworks to monitoring the impact of risk events and overseeing how management deals with material risks.

Failures and misconduct arising from lack of oversight of non-financial risk in financial services institutions suggest that greater focus and time needs to be dedicated to these challenges.

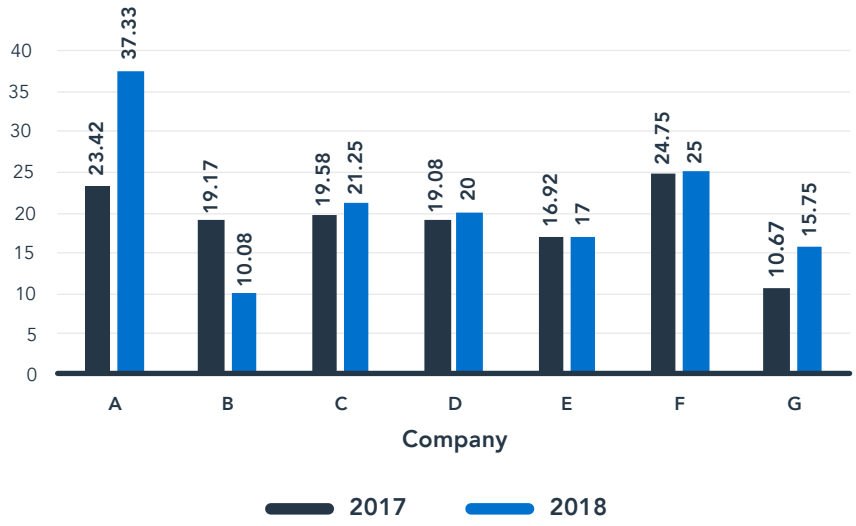
The chart below shows the total annual sitting hours of the BRCs of the companies reviewed.

Given the complexity and scale of these companies, the total hours spent sitting each year seems modest, especially considering the events faced in 2018 (including the Financial Services Royal Commission). Some companies held additional board meetings rather than BRC meetings to deal with ad hoc issues requiring board-level discussion or decisions. But we are still concerned about the limited sitting time of BRCs, considering the breadth of their mandates and the challenges these companies face in relation to overseeing and managing risk.

Despite committees often being referred to as the 'workhorses' of boards, the total overall time spent for most companies suggests:

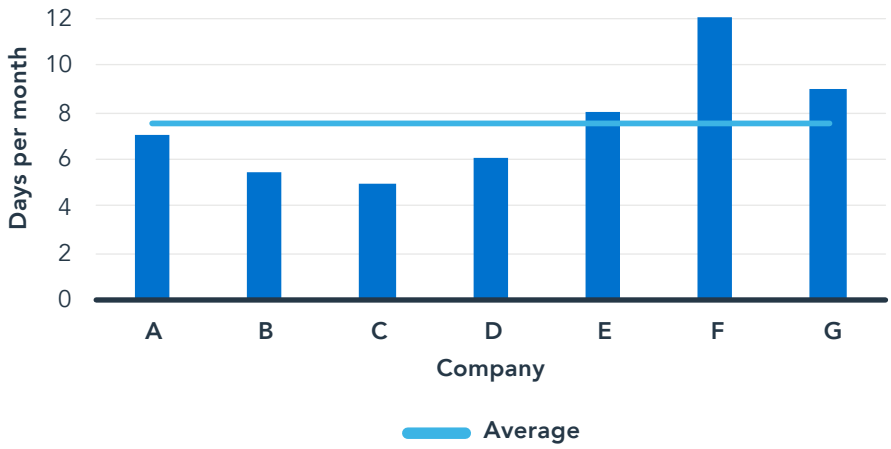
- BRCs are not considering significant risks, which are being dealt with at other venues such as full board meetings, and/or
- BRCs are not being fully utilised to resolve the challenges non-financial risks represent to companies.[41]

Total annual hours for BRC sitting



41 See **Attachment A** at page 5 for discussion regarding reflective thinking time.

Estimate of time commitment as a BRC chair and non-executive director – days per month



As the chart above shows, BRC chairs estimated they needed, on average, five to 12 days a month (1.25–3 days a week) to perform their non-executive director and BRC chair roles, with many noting that the workload had increased over recent years.

In providing this average figure, many BRC chairs commented that there were times when the demands were more intense due to company reporting or other requirements. Some stated that at times they were required to be available every day to deal with matters that arose. Many noted that the events of the past 12 months had also led to periods of intense activity.

Given the observations in this report, directors who chair or sit on a BRC need to consider whether they are committing sufficient time to BRC-related duties. Most board members we interviewed held board positions on multiple companies. They need to consider whether the number of positions they hold allows them to adequately discharge their oversight responsibilities, given the size and nature of the companies and their board responsibilities.

Better practice

Committees dealing with risk need to ensure they give sufficient time to discharging their risk mandate. This includes the need to consider 'big picture' framework issues as well as current and future risk positions or significant risk events that emerge.

Directors who chair or sit on a BRC and multiple other boards should ensure they have capacity to attend to their oversight duties not only during 'business as usual' periods but also during periods of intense activity.

Boards should ask themselves:

> **Are we dedicating sufficient time to risk issues, including non-financial risks, at the BRC level?**

BRC chairs should also ask themselves:

> **Am I allocating sufficient time to perform my duties as BRC Chair, taking into account the scale and complexity of the company?**

2 BRCs need to meet often enough to oversee material risks in a timely manner

A BRC should not just be a forum to consider the company's approach to risk at a framework level. It needs to be able to oversee the company's practices to be satisfied it is following the risk management framework and that the framework is effective.

All BRC charters reviewed by the Taskforce require BRCs to oversee management's implementation and operation of the risk management framework and risk management strategy. A review of the minutes of some companies' BRC meetings indicated that the BRCs oversaw current and emerging risks, in addition to risk framework matters.

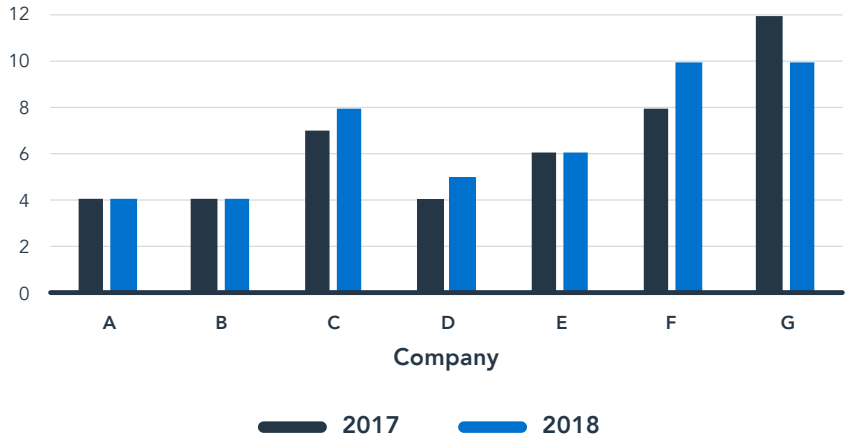
However, BRCs should ensure they are being made aware of material risks in a timely manner. This helps with identifying trends and leading indicators, to address risks earlier, reduce the severity of the impact if the risk crystallises, and identify root causes.

A BRC that meets quarterly has limited ability to respond to leading indicators in a timely manner or monitor time-sensitive issues. While time-sensitive matters can be dealt with outside the BRC, the BRC should meet with enough regularity to ensure that issues are dealt with promptly.

As the chart below shows, the number of BRC meetings each company held varied between four and 12 over 12 months in 2017 and 2018.

Standardised or repetitive items dominated meeting agendas, which were largely set at the beginning of the year. We observed that those companies that held, on average, monthly BRC meetings had agendas that included a wider range of matters that had arisen. In contrast, BRCs that met more infrequently had less varied meeting-to-meeting agenda items.

Number of BRC meetings (annual)



Better practice

It is important to identify trends or significant risks early. Two companies formalised this in their charters. One gave its BRC a mandate to 'identify thematic issues that require attention' and the other required the escalation to the BRC of 'new, heightened or significantly varying risks in a timely way'. However, BRCs need to ensure this occurs in practice and is not just an aspirational statement in the charter. We saw evidence of one BRC requesting 'deep dives' into certain risks, as a form of root cause analysis.

While it is important to have processes for escalating urgent risks, if material risks are routinely addressed outside committee meetings, companies should consider whether the frequency of their BRC meetings is adequate.

Boards should ask themselves:

> **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 BRC members need to ensure they are providing informed oversight

Without receiving adequate information, BRCs cannot identify the root causes of issues that arise, nor monitor how the company is tracking against its risk appetite. Information flows between the board, committees and management are discussed in more detail on pages 26–40.

The charter of one BRC we observed states:

> The Committee's principal function is one of supervision, oversight and monitoring. The Committee performs its principal function based on information provided to it by management. Management is responsible for the preparation, presentation and integrity of information provided to the Committee. Without limiting the Committee's responsibilities, as described in [the] Charter neither the Committee as a committee nor any member of it by virtue of being a member, has the duty to actively seek out activities occurring within the Group that are not compliant with the Group's policies and procedures, although they have a duty to act promptly if any such activity comes to their attention.

We understand this clause was included to clarify the company's understanding of the delineation between management and the board, but was to be read in light of other provisions in the charter as well as legal obligations on directors requiring active stewardship. Specifically, it was intended to deal with any expectation that the BRC members would act in the role of management in looking for issues.

However, as drafted, in isolation the clause could be misconstrued as sanctioning BRC members to accept information provided to the committee on face value, without challenging its nature or quality. ASIC understands that this company has not adopted this practice, but including such clauses in charters could be misinterpreted in this way, and does not represent good practice.

Better practice

Members of the committee must ensure they are providing informed oversight. If the BRC believes management is not giving it adequate information about compliance with the risk management framework, or if it is only receiving 'good news', then the BRC has a duty to make enquiries of management and take steps to rectify the information flow. BRCs should ensure that their charter accurately reflects actual practice in relation to informed oversight.

Getting management to undertake root cause or thematic analysis of non-financial risks that continue to arise in the company's operations demonstrates active stewardship on the part of directors. These enquiries are for the purposes of informing the BRC, not undertaking the role of management.

Boards should ask themselves:

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

4 Boards need to actively engage in decisions and proposals at the BRC level

Active stewardship means directors cannot simply sit back and accept information provided on face value. They cannot, as one director noted, just 'look to them [division head] to tell us if they're managing their business properly'. Directors should actively probe and analyse information presented by management to test its robustness, and judge the merits of proposals and the adequacy of management actions.

We consider that signs of active oversight include directors:

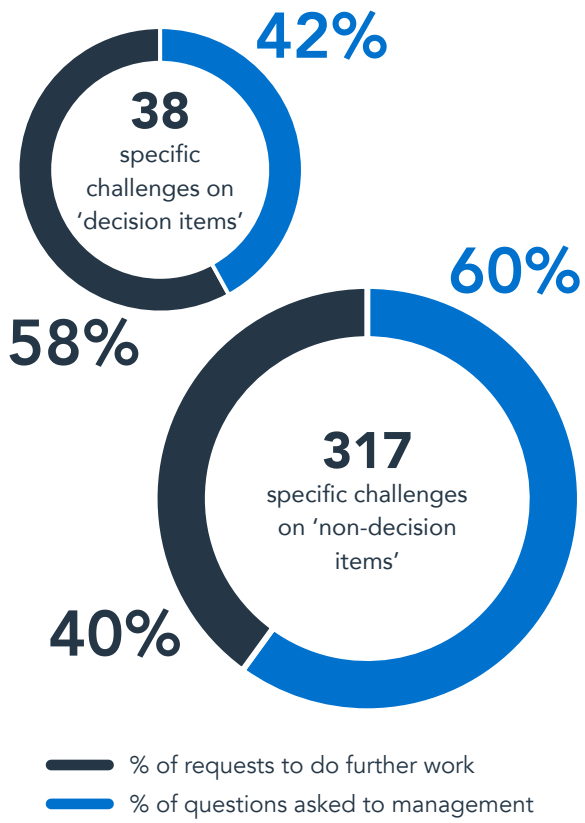
- requesting further information, analysis or action from management
- asking questions of management
- requesting changes to recommendations or proposals
- rejecting recommendations or proposals
- driving the implementation of changes to address identified failures by management.

Our assessment of the existence of active oversight relied on our review of BRC minutes. These minutes were typically very high-level, so the data below needs to be considered in that light.

We observed from minutes of BRC meetings in 2018 that there were more instances of active oversight of non-financial risk matters than of financial risk matters. This could be explained by the nature of the subject matter, greater focus on these matters recently and a conscious decision to capture these issues in the minutes.

There were signs of active oversight in only 29% of all items that required a decision, and in 32% of 'non-decision items'.[42] As shown in the infographic below, of the items that needed a decision, the board required management to do further work or implement changes in a higher proportion of cases than for the 'non-decision items'. The majority of board engagement in relation to 'non-decision items' consisted of the BRC asking questions or requesting further information.

BRC challenges



42 Items requiring a decision included items for approval. 'Non-decision items' included items for noting, discussion and consideration. The review did not measure the number of times the same matter was brought before the BRC.

Active oversight requires directors to take action to prevent failures from reoccurring rather than merely expressing concern. In a single board meeting for one company, we observed three separate requests for board ratification due to management's prior failure to seek board approval at the required time. In each instance, the minutes record that the board 'expressed concern' over the failure to seek board approval at the relevant time, yet nevertheless ratified the action. In two of these instances, the board also identified a delay in seeking ratification once the failure had been identified and on one occasion the board merely 'reiterated the importance of escalating bad news quickly'.

This example demonstrated a lack of active engagement by the board with the very serious issue of an apparent systemic lack of compliance with key internal controls relating to board delegations, as the board did not appear to take ownership of the issue. Instead of the board instigating and driving a review into how their delegations were being managed, the delegates themselves appeared to drive the scope of the internal review into the problem. While this conduct occurred at a board meeting rather than BRC, we would expect a similar level of active oversight by the BRC.

Better practice

Asking questions of management is good practice. But simply expressing concern, or passively providing feedback for management's 'consideration', is not the same as genuine active oversight. Such oversight can involve changing behaviours and imposing consequences, where necessary. This is especially so where the board or BRC sees evidence of systemic issues (for instance, the continued failure of internal controls that result in not seeking board approval).[43]

We did observe instances of boards providing active oversight:

- One company introduced a requirement that accountable executives from the responsible business unit attend board meetings to talk to high-rated 'red' risk incidents and to take responsibility for closing them out.
- Where the board expressed concern over a particular course of action, we also observed an example of members asking specific questions about methodology, managing consequences and the adequacy of resourcing before requesting updates on progress and changes to reporting.

Boards should ask themselves:

> **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?**

43 See **Attachment A** at page 4 for discussion regarding boards challenging management.

5 There should be clear escalation processes for urgent material risks

There should be clear and effective processes to escalate and deal with urgent material risks that arise between BRC meetings. Dealing in an ad hoc manner with time-sensitive issues that are sufficiently material to be escalated to the BRC can result in:

- no consistency in the matters escalated
- fractured information flows to the board
- board members only partially participating in significant decisions
- issues not being followed up appropriately.

The charter of one BRC set out a procedure for addressing time-sensitive issues arising between BRC meetings, which listed possible alternative decision makers and how the BRC would be notified. Nevertheless, ASIC observed that this company adopted alternate practices in some instances, such as the board Chair calling all board members to discuss a matter.

In fact, we observed different practices adopted within companies and between companies in response to urgent risks, including:

- discussions between the CRO and the BRC chair. In some cases BRC chairs would then notify the remaining BRC members by phone or email. The matter may also be placed on the agenda of the next BRC
- direct communication between the CEO and board chair
- impromptu board or BRC meetings
- in the absence of a BRC meeting, escalation of urgent issues to the next monthly full board meeting
- for urgent risk matters arising through an audit, impromptu discussions between the board audit committee chair, board chair, BRC chair and CEO.

The variety of processes within and between companies indicates there is no standard process for escalating urgent material risks – either within each company, or across the financial services industry.

Better practice

Different circumstances may warrant different responses. What is important is that there should be transparent and consistent processes for escalating urgent material risks outside committee meetings. These should detail who, where and how to deal with and close out these issues.

Transparent escalation processes should define:

- who to escalate the matter to initially (the BRC chair, the CEO and/or the board chair)
- the forum for addressing the issue and how to involve BRC members (for example, hold an ad hoc BRC meeting or full board meeting, or have the BRC chair and CRO reach a decision, which is then communicated to other BRC members)
- how issues are recorded and closed out so the BRC retains oversight if these matters will not be captured in the action items register of regular committee meetings.

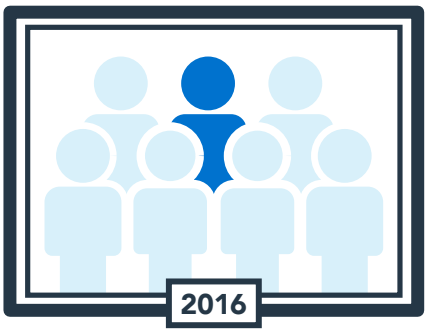
Boards should ask themselves:

> **Do we have transparent and effective processes for escalating urgent material to the board?**
>
> **Are these processes followed consistently?**

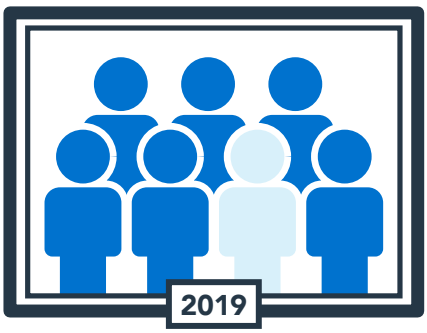
6 Emerging issue: Implications of changing BRC membership and attendance patterns

We observed an emerging trend in which all non-executive directors are increasingly invited to BRC meetings (see infographic below). While in two of the six companies all non-executive directors were members of the BRC, we observed that in six of the seven companies all non-executive directors routinely attended BRC meetings.

BRC attendance



1/7 of the companies reviewed had the full board routinely attending



6/7 of the companies reviewed had the full board routinely attending

Interviewees noted that having full board attendance had advantages:

- There was less need to repeat issues to the full board.
- Nothing was 'lost in translation' as all directors were informed about all areas, helping them make other general board decisions.
- It freed up the full board to focus on strategy.

Some interviewees cited disadvantages:

- Having all directors in the room stifled conversations and did not allow deep dives into topics because there were too many voices.
- Full board attendance was likely to lead to a 'good news culture' in reporting as 'the better the audience, the better the news'.

Where all non-executive directors attend BRC meetings, there are potential unintended consequences, such as a lack of voting rights for directors who are not members.

Better practice

Companies with full board attendance at BRC meetings should consider their motivations for establishing such a practice. If a company has inefficient information flows, resulting in the full board having to attend BRC meetings, the company should also prioritise improving its processes.

Where a company decides to have all directors attend BRC meetings, it would be better practice to formalise this decision by making all directors committee members. This would ensure that attending directors have the requisite voting rights, so they are not disenfranchised from material risk decisions.

Formalising membership also reduces the risks involved with informally reducing information flows to the full board in circumstances where directors may stop attending BRC meetings at any time.

It is also essential for companies to have an effective BRC chair who retains control and carriage of BRC meetings. This is more likely to maintain structured and robust decision-making frameworks and accountabilities, regardless of membership and attendance.

Boards should ask themselves:

> **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?**

International trends

In the United Kingdom, large listed companies are required to establish a BRC that takes primary responsibility for risk management. In other prominent international jurisdictions, risk committees are also gaining traction outside financial services.

In relation to boards and board committees holding management to account, the Canadian regulator expects financial institutions to provide evidence in meeting minutes that boards are effectively challenging management. While this has led to more rigorous documenting of challenges, it is also likely to focus the board's attention on ensuring that effective challenge occurs.

Globally, first-line business units (in the three lines of defence model) are increasingly participating in, owning and being held accountable at board level for risk management. Many entities are reviewing and refining their governance structures, focusing on the first line presenting the business unit's risk profile to the board, rather than the second line (the risk function) performing this task.

Appendix 1: Board questions

Boards of all large ASX-listed companies should consider the observations set out in this report and ask themselves the questions outlined. These questions are replicated below.

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: Methodology

The Taskforce employed a multi-disciplinary approach to its governance review, including document review and interviews with directors and officers.

Document review

The initial stage was a document-based review. ASIC used its compulsory information–gathering powers, issuing notices on all companies pursuant to s33 of the *Australian Securities and Investments Commission Act 2001* (ASIC Act). In total the Taskforce received more than 29,000 documents for review (which included some documents to assist the Taskforce's review of executive remuneration).

The material included agendas, papers and minutes of selected BRC meetings and board meetings.

This material was reviewed with the assistance of a hypothesis-led review methodology. Deloitte provided ASIC with a methodology, which was adapted by ASIC for the purposes of the review.

This methodology focused on several governance themes and helped the Taskforce to identify good and poor governance practices across the documents being reviewed.

These themes covered board structure for monitoring and supervising; risk governance; board and management accountability; reporting and information flows; and risk resourcing.

The review was conducted by ASIC. Deloitte were not otherwise involved in the review and did not participate in any inspection of documents or interviews of participants.

Voluntary interviews

The Taskforce also conducted 60 voluntary interviews with executive officers and directors of companies, to deepen our understanding of the practices the Taskforce had identified from the document review.

Interviews with officers and executives included companies' CROs, chief audit executives and secretaries. Interviews with directors included the CEOs, BRC chairs and board chairs.

Behavioural analysis

The Taskforce's report looked at the oversight of non-financial risk, specifically issues regarding the use of risk appetite statements as an oversight tool; information flows between management and directors; and the role of the BRC in the oversight of non-financial risk and root cause analysis.

Behavioural interactions between members of the board and between board and management are relevant to the effectiveness of this oversight.

To assess how board behaviours enhance or impede their oversight and monitoring role, the Taskforce commissioned behavioural analysis from behavioural experts, Kiel Advisory Group.

Kiel Advisory Group interviewed directors and officers of six large listed companies including financial services and non-financial services companies; observed five board meetings and three board committee meetings; and undertook a targeted document review in relation to these companies. Survey responses from a wider cohort of 19 companies (including the six 'deep dive' companies) also assisted in informing the analysis. The behavioural analysis included the preparation of a thematic report by Kiel Advisory Group on board behaviours and how these can influence board oversight of management of non-financial risk. This report is set out in **Attachment A**. The purpose of this report is to provide additional guidance and insight to boards, and to highlight strategies they could implement to address the effectiveness of their oversight.

International practices

ASIC procured research from Deloitte into international governance practices relating to director and officer oversight of non-financial risk in the United Kingdom, the United States, Canada and Germany. This research identified global trends in corporate governance, next to which we could compare the practices we observed in our review of Australian organisations.

Deloitte provided comparative (publicly available) data across a sample of 40 large listed companies within these jurisdictions, along with insights on jurisdictional better practices from its international subject matter experts.

Individual company feedback

At the conclusion of the Taskforce's review, individual written feedback was given to the CEO and chair of each company that participated in this review to directly drive improvement of the company's practices.

The Taskforce provided feedback on good practices and those that boards should change to improve their oversight of non-financial risk. Individual feedback sessions with the CEO and chair of each company will also be undertaken.

ASIC Corporate Governance Taskforce
Director and officer oversight of non-financial risk report

asic.gov.au