ORGANISATION

The evolving role of the risk committee

The Australian and international risk landscape has undergone a transformation in recent years, accelerated in 2020 with the COVID-19 pandemic. Whilst the focus post global financial crisis centred very much on financial strength and financial risk, there is no doubt that non-financial risk has now moved squarely into the central frame and sits with equal importance for the wellbeing and long-term sustainability and success of an organisation. These developments have resulted in Australian companies today operating in a dramatically different economy and social environment – and hence a significantly evolved risk matrix.

This year alone we have seen the devastating and immediate impact non-financial risk can have on a company's reputation and value, with examples of sexual harassment, bullying and cultural insensitivity resulting in irreversible devastation. Furthermore, climate change, digital transformation, AI technology and cyber security all highlight how business sustainability in the broadest sense is now recognised and demanded – giving rise to both new risk and new opportunity. Many of these issues go to the very heart of the culture of an organisation and they are now on the radar of many stakeholders: employees, shareholders, investors, regulators and communities in which a company operates. Voices are being raised and muscle flexed.

Recent corporate scalps have been large and high profile, but they reflect relevant issues and challenges for organisations of every size and in every sector. Many of them stem from human behaviour and a healthy culture is the only true safeguard for this, along with strong governance. Assessing the strength and health of workplace culture can be challenging and it is important to set up the right framework to do so. The risk committee plays a very important role here.

Many of these non-financial risks can be very tough to truly identify, measure and address – particularly for boards, with their limited line of sight – but they must be. So how can boards and risk committees bring best practice to try and identify, assess, measure and monitor these risks effectively? And how do they do so in addition to the risks posed by COVID-19 and the financial risks they must still keep front and centre? In other words, how does the traditional risk committee need to evolve to do its job properly and to help their board have the eyes and ears needed to ensure that management is not just keeping within the set risk appetite, but managing risk effectively to protect the company's reputation and value and, ideally, create opportunity?

COVID-19 has forced proactivity

As the COVID-19 pandemic took hold in 2020, organisations were immediately placed into crisis mode. New and immediate risks emerged, and continue to do so today, stress testing existing risk frameworks.

This has resulted in companies facing a risk environment more complex than most could have imagined only years ago. In turn, this has put a spotlight on the role of the risk committee in helping both the board and management to 'manage' risk effectively.

A holistic approach to risk can create sustainable growth. It can achieve goals safely, enhance innovation, build business resilience. Approaching risk proactively rather than reactively – gathering useful data early and identifying risk insights and trends – allows good strategic decisions to be made. It can also prevent huge financial consequences. Think of the billions of dollars spent recently in the financial services industry on remediation costs.

A failure to deal with risk appropriately, particularly non-financial risk, has been a factor in the breakdown in public trust toward business. The Edelman work on trust shows this clearly.[1] To rebuild and regain that trust, boards and management need to align on the broadened risk environment. It is vital to evolve the way organisations identify, manage and report on risk.

The risk environment is complex

In addition to the rise in prominence and importance of non-financial risk post Hayne Royal Commission, certain risks have been exacerbated and risen to prominence during COVID-19 and will continue to need special attention. By way of example: crisis management; heightened insolvency and reporting risks; new government regulation; dispersed workforce culture; COVID-19-related WHS, mental health and employee wellbeing; heightened cyber risk with working from home; supply chain exposure; change in competitive landscape; overall organisational resilience; diversity and inclusion regression[2]; increased demands from activist shareholders/proxy voters; speed of digitisation/move to the cloud; geopolitical risk (return to insularity and its impact).

The above is all in addition to existing and continuing financial, operational and compliance risks – further compounded by, as already mentioned, some extreme conduct risk bubbling very publicly to the foreground this year.

This environment is very complex and the range of risks is diverse and difficult to navigate. Non-financial risk management requires quite different skills to financial risk management. It is therefore important for organisations to assess their existing risk management skill base for its ability to cope and adapt as necessary.

The financial loss resulting from not managing risk well can be direct and substantial. What has been increasingly recognised over the past few years is the significant reputational damage that can also be caused and the dire impact this can have on the overall value and the sustainable health of a business.

Back to fundamentals

For the risk committee to have proper oversight, all decisions around how to manage risk must start with a clear understanding of what is the organisation's risk appetite. This is a question every board should be revisiting right now – in light of COVID-19 and the (in some ways drastically) changed societal, economic and risk environments now facing their organisation.

From that point, the questions of 'who?' (responsibility and accountability) and then 'how?' can also be looked at afresh. Recent events have shown it is important to be proactive in resetting these fundamental questions and not waiting for something significant and potentially damaging to first occur.

So why is the risk committee now more important than ever? When working well, an effective risk committee can:

- help bring independent judgement to risks;
- help focus the board on its oversight of non-financial risk and its increasing importance;
- review and debate risk appetite and frameworks;
- monitor compliance with risk appetite and tolerances;
- monitor material risks including emerging ones;
- deliver a deep dive on issues in a way the board itself cannot;
- ensure the escalation of significant incidents and breaches; and
- identify root causes and trends.

Just how complex the environment is and what must be navigated illustrates vividly why the role of the risk committee must be seriously looked at and continue to be constantly reviewed and evolved to adequately play its role in helping the board fulfil its important governance duties.

[1] Edelman, *Trust*, [website], **https://www.edelman.com/trust**, (accessed 10 Nov 2020).

[2] J MacKay, 2020, *COVID-19: Inclusive leadership in times of uncertainty*, PwC Australia, 31 March, **https://www.pwc.com.au/important-problems/business-economic-recovery-coronavirus-covid-19/inclusive-leadership-times-of-uncertainty.html**, (accessed 16 Nov 2020).

Taking a holistic approach by integrating risk into strategy and culture

For the risk committee to have confidence in being able to fulfil its function, the way the organisation manages risk is critical. Risk management can often fail because it is removed from the frontline. There can be a divorce between operations and risk. This can make it very difficult for management, and hence the risk committee, to truly understand what is happening on the ground. This was highlighted quite dramatically in the many issues (including anti-money laundering risk) faced by the banks over the last three to four years. So how to avoid this divorce? What should the risk committee be looking for?

A cohesive, integrated approach to risk is crucial to ensure responsibility and accountability are clearly defined and understood. The risk committee must have enough line of sight into the practice on the ground to be satisfied this is taking place. While many companies have invested heavily to manage non-financial risk better – increasing headcount, creating new governance structures, making operational changes – mitigating non-financial risk remains difficult. There is often no direct warning of when or where the next non-financial risk might materialise.

The size of an organisation may dictate the level of sophistication of its risk framework, but it is more and more common in developing an enhanced non-financial risk governance framework to put in place the Three Lines of Defence model:

- Line One: the business unit that owns the risk manages it;
- Line Two: the risk and compliance unit – now often extended to also include other units such as HR, legal and finance – sets control standards and monitors adherence to them; and
- Line Three: the audit function keeps a check on the adequacy of the first two lines.

The effective implementation of this model can be much harder than it sounds. Responsibilities between the first and second lines can become blurred. Business units/ control functions can be siloed with each having its own risk identification processes, reporting structures and IT systems. This can make the role of the chief risk officer (CRO) very difficult and they can often struggle to provide the risk committee/ board with a thorough view of risks faced and controls required. Streamlining and simplifying the structure by eliminating overlap and making clear decisions on responsibility within the framework is important – one person being responsible for the whole risk across the entire organisation, or a decentralised model or a combination of both). Risk committees must be alive to this.

What is important is to define a consistent set of principles and language that reflect the governance structure, operational complexity and the specific regulatory requirements of the organisation. The risk committee should satisfy itself of this.

These principals need to emphasise that the first line units must take responsibility for non-financial risk management and not just focus entirely on revenue and/ or cost management. This is important to ensure that risk management controls are at the front of senior management and employees minds, allowing a consistent and embedded risk framework through all levels of the organisation. This first line responsibility for non-financial risk management is what the risk committee should aim for and seek to monitor and measure. Commentators on the events that transpired at Rio Tinto this year have observed the negative impact that was likely had in placing indigenous cultural matters within corporate affairs – it did not have the prominence and importance it needed.[3] Framework is important.

Finally, and critically important, is culture. However strong the risk framework, management of non-financial risk will fall short unless it is supported by a culture led from the top down that acknowledges its importance. Having the risk function work collaboratively and share the same language with senior management and the business units will help raise the non-financial risk profile and ensure it is considered when the business is developing its strategic plan. It will also ensure it is embedded within the culture. The APRA self-assessments following the Hayne Royal Commission emphasise that the regulators are also recognising this and have started to pay much more specific attention to risk culture.[4]

[3] J Hewett, 2020, "Rio Tinto's detonation of trust adds up", *Australian Financial Review*, 28 July, **https://www.afr.com/companies/mining/rio-tinto-s-detonation-of-trust-adds-up-20200728-p55ga5**, (accessed 16 November 2020).

[4] Australian Prudential Regulation Authority, 2019, *Information Paper: Self-assessments of governance, accountability and culture*, 22 May, **https://www.apra.gov.au/sites/default/files/information_paper_self-assessment_of_governance_accountability_and_culture.pdf**, (accessed 16 November 2020).

Ten tips for increasing the value of the risk committee

The size of the company, and of the board, may determine whether to have a standalone board risk committee or whether it is combined with another function like audit. A dedicated risk committee is the strongest option as it ensures that risk, and instilling a risk culture, is elevated to the important place it needs to be and has the focus that it deserves. And given how multi-dimensional and complex the risk landscape is, for many sizable organisations, a committee would struggle being able to effectively deal with anything but risk alone.

Set out here are a number of practical tips and good practices for risk committees to think about and adopt. The Australian Securities and Investments Commission (ASIC) recently published its observations around board risk committees and what better practice would look like in its *Director and Officer Oversight of Non-Financial Risk Report*.[5] Although aimed at listed companies, there are a number of practical recommendations with much wider application, some of which are included here in summary as well:

1. Dedicate enough time

The importance of dedicating sufficient time is particularly the case for the role of the risk committee chair. The risk committee's role is one of active involvement, not box ticking. Statistics obtained by ASIC show not enough time appears to be dedicated. This highlights the question of how many boards a director can effectively sit on, particularly if they chair the risk committee.

2. Meet often enough

To oversee all material risks in real time – more important than ever in this era of COVID-19 – the risk committee has to meet often enough. The role of the risk committee is not just to look at the framework but to actually oversee its practice, to be satisfied management is acting within the risk appetite and to confirm that the risk management framework is sufficient. The risk committee needs to identify trends and leading indicators to address risks earlier, reduce the severity of their impact and, importantly, identify root causes. This can be difficult and time-consuming, so it is important that the risk committee meet frequently enough to do so.

3. Ensure there is sufficient information flow

The risk committee needs to have sufficient information in order to provide informed oversight. Breadth and materiality are key. It is important to seek action-oriented reports that align to a clear definition of the risk appetite. This is to help have a forward-looking perspective of the top risks, to assess the adequacy of the control systems, conduct the thematic analysis of the issues that keep arising, to keep within agreed risk tolerance boundaries and then to ensure that any control gaps are addressed. It is also important to ensure the right and timely flow of information is set up between the board, the risk committee and senior management.

4. Maintain active oversight

Active oversight means probing and analysing management in order to test for robustness. The risk committee must help the board take action to prevent failures reoccurring. It is about changing behaviour and imposing consequences – and not just about expressing concerns – particularly if it is a systematic issue. Good practice does not just accept good news. Good practice is also not afraid to bring before the risk committee whoever is necessary from within the business unit, or another second line function other than risk/compliance, to explain and then help close out risks. This will help bring the risk committee/board closer to the business.

5. Establish clear escalation processes for urgent material risks

The COVID-19 crisis reinforced the importance of processes for escalating urgent material risks. Dealing with sensitive issues in an ad hoc manner without clear process can be dangerous. The board risk charter should set out the timing and who should be contacted if a matter is objectively urgent, and then the process for recording and closing out such risks when dealt with. There may be different approaches by different organisations depending upon size and complexity, however transparency and consistency are key.

6. Keep the committee membership relevant

As an emerging issue – particularly relevant in fast-changing and complicated times – risk committees must think of the implications of risk committee membership refreshes and attendance patterns. The trend has been to invite all NEDs to be members. This is good practice. Consider whether they should all be members as well, so as not to confuse on who has voting rights. Be conscious of size – if the risk committee is too large it can become ineffective (particularly at deep dives) and unable to be as nimble as a risk committee needs to be.

[5] Australian Securities and Investments Commission Corporate Governance Taskforce, 2019, *Director and officer oversight of non financial risk report*, October, **https://download.asic.gov.au/media/5290879/rep631-published-2-10-2019.pdf**, (accessed 11 November 2020).

7. Make minutes relevant and check cross-committee information sharing

Make sure minutes capture all key discussions, decisions and reasons. Check how closed sessions get minuted. Check how absent committee members are updated and action items are conveyed to the board and management. Formalise how cross-committee information sharing will take place, as it is important to ensure an integrated wholistic approach functions well.

8. Harness technology for better data and measurement

Measurement is important. Measuring non-financial risk is hard but the risk committee should satisfy itself that best data is being collected, analysed and presented. Advanced data analytics – combined with the analysis of a broader range of data – can deliver improved outcomes such as catching unauthorised behaviour, reducing employee turnover, improving hiring decisions, reducing fraud rates, better detecting of specific suspicious transactions and so on, all with fewer resources.

Harnessing and using data can also be used to identify potential risks early and proactively make good decisions to protect the organisation. Technology-enabled processes and systems (for example, utilising big data, predictive analytics, AI, etc.) help the risk committee, board and management to understand what is happening across the business, measure performance against risk appetite, and develop much greater insight into emerging patterns, trends and root causes. This means risks can be identified early rather than when a catastrophic event surfaces. How much can be invested in early-warning frameworks will depend on the size and complexity of the organisation but it is a relevant consideration for all.

9.Update the risk committee charter and keep it simple

It is good governance practice to regularly embed refreshed practices into the risk committee charter. This ensures clarity on the role and responsibility of the committee, its composition, structure, membership, authority processes and procedures and evidences clear board approval. The charter should reflect practice – embedding will encourage and help ensure that what is agreed happens in practice and doesn't end up as only an aspirational statement. Avoid unnecessary complexity and keep the language simple.

10. Establish constructive relationships with board and management

In the past few years following the Hayne Royal Commission, there has been significant conversation on the impact of behaviours and relationship on effective governance, including the merits of placing psychologists in the boardroom. And for good reason. Good constructive behaviours and relationships between the risk committee/ board members and management can significantly enhance the proper management of risk – in particular, non-financial risk. But if they are poor, they can significantly impede it. It may be useful to consider getting independent external help to assess your behavioural and relationship score card and to suggest ways to improve.

The importance of the C-suite in protecting reputation and value

The board's responsibility for governing today's broad risk landscape – whether with or without the formal function of a risk committee – can also be well supported by a perceptive C-suite.

Structuring roles, responsibilities and reporting lines so as to allow them greater access to see how the organisation's non-financial risks are playing out at ground level, can bring a fresh perspective on how to protect reputation and drive value. Visibility, communication, transparency and accountability provide a safe, speak-up environment, which is important to ensure employees will share relevant and telling information, and crucial for important learnings.

While one-off incidents and clearly defined risks tend to be more easily captured, reported and managed through traditional risk frameworks, paying attention to how the C-suite is structured and who has responsibility for certain risks and who they report to, can also give the CEO (and through them the board) a measure of evolving and as-yet intangible risks, many of which may be a real indicator of overall cultural health. The aim is to think outside the square and achieve a 360-degree view and a deep line of sight.

About the Author

Tricia Hobson GAICD is a litigation and insurance lawyer based in Sydney and a partner at Norton Rose Fulbright. She is a leading Australian class action lawyer accountable for leadership, strategy and negotiations for four of the largest class actions in Australia. Tricia is past Global Chair of Norton Rose Fulbright.

About us

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

For more information **t:** 1300 739 119 **w:** aicd.com.au