Risk governance and culture

By Associate Professor Elizabeth Sheedy PhD, Macquarie University Applied Finance Centre

- 'Risk governance' has emerged as a new governance paradigm which better serves all stakeholders.
- If risk governance is implemented due to regulatory pressure rather than by choice, it may be undermined by poor risk culture.
- An effective assessment of risk culture needs to not only assess the structures of risk management but also reliably measure the perceptions of employees.

Risk-taking is inevitable and even desirable both in business and in life. As every entrepreneur knows, only by taking risk can great things be achieved. Taking the right amount of the right risks is arguably the main task of senior leaders and so the goal of risk management is not to eliminate risk but to increase the odds of achieving the desired outcome.[1]

Coming from a finance background I believe that risk-taking works when:

- the risks are understood by all the stakeholders who will bear the consequences of risk-taking
- the expected return for bearing the risk is considered acceptable by those stakeholders, and
- mitigants and controls, appropriate to the context and risk appetite, have been established.

So why has risk become such a hot topic in governance circles? Firstly, the extent of risk-taking is often *not* well understood by senior leaders. The statistical models typically used for analysing risk are useful but incomplete descriptions of reality. The models themselves can be difficult to understand because they use mathematical/statistical concepts that are demanding for those who are out of practice with (or have never previously been exposed to) such concepts. Second, risks are often hidden, obscure or understated. This can occur either through oversight, laziness or, more worryingly, with intent. There are many individuals/groups that have incentives to hide or minimise the risks they are taking. Finally, humans seem to have difficulty interpreting information that relates to risk. They make cognitive errors that seem to result in many of the same mistakes being repeated over time. For example during extended periods of prosperity, disaster myopia sets in; senior leaders may become over-confident in their ability to withstand adverse events.

Risk governance: What and why?

'Risk governance' has emerged as a new governance paradigm which, through greater emphasis on risk management, better serves all stakeholders (not just shareholders). The underlying premise is that by increasing the focus of the board on risk management and elevating the status of risk executives, risk will be better managed leading to fewer surprises, scandals and insolvencies. In the long run, firms with strong risk governance should achieve higher risk adjusted performance (although not necessarily lower risk as some firms may legitimately choose a high risk appetite).

The governance structures typically discussed are: presence of a chief risk officer (CRO), CRO access to board, CRO status and authority (evidenced by presence on the most senior executive committee and total remuneration comparable to other senior executives), and presence of a board risk committee which is active and includes independent and experienced directors.

So how might better risk governance lead to better organisational outcomes? Risk governance might allow senior leaders to better quantify and manage the risk-return trade-off at the firm level, for example, by finding and exploiting natural hedges within the firm or by creating a diversified portfolio of businesses. A well governed firm should have the processes to identify the optimal amount of risk that maximises value subject to regulatory and legal constraints, and to ensure that the actual risk is consistent with this optimal amount. Such a firm is more likely to invest in a risk-taking *framework* (to ensure that risk is measured, monitored and managed throughout the organisation) and risk-focused *remuneration* systems (that reward managers for creating value while holding them accountable for taking risks that destroy value). With risk governance a firm is likely to develop a strong and independent risk management function. This adds value by restraining staff who might take excessive risks for personal benefit (such as short-term bonus payments).

A well governed firm should have the processes to identify the optimal amount of risk that maximises value subject to regulatory and legal constraints, and to ensure that the actual risk is consistent with this optimal amount.

Risk culture: What and why?

Having the trappings of risk governance (such as a high status CRO) clearly does not guarantee that risk will be well managed. Indeed the very success of the risk governance movement may threaten its efficacy as risk governance can now be considered a requirement in some industries (especially financial services).

If risk governance is implemented due to regulatory pressure rather than by choice, it may be undermined by poor risk culture that is, lack of any genuine commitment to risk management. Staff within the organisation will easily ascertain the true priority accorded to risk management and behave accordingly. Indeed, humans are adept at discerning the real priority of the organisation; they do this through all forms of communication (including non-verbal), not just what appears on the company website. They will typically be strongly influenced by respected peers and management at the local level in forming these perceptions. For example, if they observe that top performers in their team are rewarded despite breaching risk policies, employees will conclude that risk management is a low priority.

Culture refers to 'the real priority around here' — staff perceptions regarding the behaviours and practices that will be most valued and rewarded. The priority could be short-term profits, customer service, innovation, safety; all of these focused climates have been researched by scholars. Research into risk culture is a new endeavour and at Macquarie University research encompasses cross-disciplinary team of experts in financial risk and organisational psychology. We have developed the world's first risk culture survey instrument that has produced evidence of reliability and validity.[2] We define risk culture as the *shared perceptions among employees of the relative priority given to risk management, including perceptions of the risk-related practices and behaviours that are expected, valued and supported*.

It's important to note that risk culture is very different from risk appetite. A firm may choose for good reasons to take high risks but this does not mean that they have a poor risk culture. If that high risk appetite is understood and respected by staff then risk culture may be favourable. Indeed one could argue that the more risk you take the more important it is to have a strong risk culture, just as a fast car needs good brakes.

Assessing risk culture

A common but flawed approach is to assess the structures of risk management, for example, the policies and systems in place related to risk management. While examining risk structures can be a very useful exercise, this is not an assessment of risk culture. As noted above, risk culture has to do with the perceptions of employees, so any assessment of risk culture will need to assess these perceptions. A firm might have best-practice risk structures but if risk culture is unfavourable, the structures will not be as effective as they ought to be.

Another important consideration is the fact that culture develops locally as explained above. Our research has shown that business units in the same firm can have significantly different culture so assessment should be conducted at the business unit level. One certainly cannot assume that the risk culture in one part of a firm will be reflected throughout.

There are a number of possible methods for assessing risk culture:

1. **Employee surveys** These can be very cost-effective in a world of secure online survey platforms. Crucially, if implemented carefully and using an independent assessment provider, they offer employees anonymity. Anonymity is essential in order to encourage staff candour. Employees will have a good sense of the true priority in the business but very few are brave enough to be whistleblowers. If you are going to use a survey then it is best to use an instrument with evidence of reliability that has been through a robust development process. Designing effective survey questions is difficult, especially

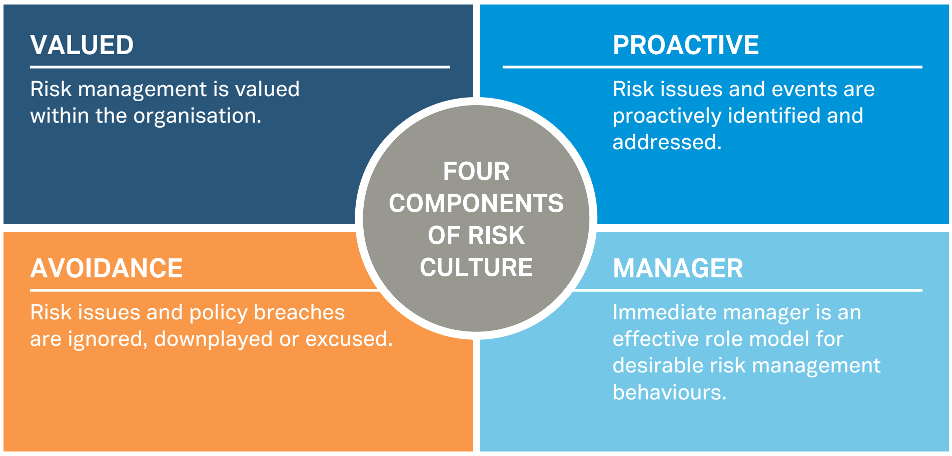
in the case of risk culture which is quite an abstract concept. The Macquarie University Risk Culture Scale™ has been through the process of academic peer review and at the time of writing has been used to assess risk culture in ten organisations with more than 35,000 individual survey responses. Not only is benchmarking available, but users can have some confidence that the survey measures what it purports to measure.

On the downside, surveys are so commonly used these days that there are concerns regarding survey fatigue and loss of employee productivity; for this reason surveys should be used sparingly. There are also concerns that employees might 'fake good' in the survey setting in order to please managers or avoid unwelcome scrutiny and/or interference in their business. This can be addressed (at least in part) by genuinely providing anonymity and by using well-designed survey questions where the 'socially desirable' answer is not obvious.

2. **Interviews** Interview methods can offer considerable insights but require a skilful interviewer and therefore implementation is very costly. An interview does not offer anonymity so employees may not be willing to share their true perceptions. A further problem is that it is difficult to make comparisons both between teams and over time because of the subjectivity of the interview process. One possible way forward is to use a survey to identify business units where risk culture is less favourable, then use the interview method to investigate the matter more thoroughly, that is, a deep dive.

3. **Internal audit** Auditors are increasingly being asked to assess risk culture using objective data they have collected such as risk events, near misses and policy breaches. One of the difficulties here is that as risk culture improves, the rate of reporting of risk events tends to increase. It can be very difficult to disentangle the reporting effect from a true increase in risk events. Some compliance departments and auditors have proposed key culture indicators for which data can be collected. For example, to examine the minutes of formal meetings to determine how frequently risk was discussed (or at least minuted). The danger here is that whatever indicators are chosen, staff will inevitably change their behaviour to ensure that performance appears superficially acceptable. But if the fundamental risk culture is flawed, problems will inevitably show up elsewhere. Such a 'compliance' approach to risk culture may therefore miss the underlying issues.

Figure 1: Four component of risk culture



What do we know about risk culture?

Over the past three years I have led a research project (funded by the Centre for International Finance and Regulation, together with Macquarie University) looking at risk culture in Australian, British and Canadian banks.[3]

- We identified four dimensions or factors of risk culture as illustrated in Figure 1.
- Avoidance is the area where banks tend to have the least favourable scores.
- Even in banks with best practice risk governance, risk culture varies to some extent at the local business unit level. So don't assume that your risk culture is consistently favourable just because you have adopted risk governance; assess culture at the local level.
- Senior leaders tend to have a significantly more favourable impression of risk culture than staff generally. This is consistent with our finding regarding Avoidance, that is, senior leaders may not be getting the full story. This is one of the reasons why an independent risk culture assessment (where staff feel able to share their true opinions) can be very valuable.
- Where risk culture is favourable, risk behaviour[4] is better. In other words there is more desirable behaviour (compliance with policy, reporting risk events, sense of accountability for risk) and less undesirable behaviour (gaming of controls, overconfidence).
- Some personal characteristics are also important for explaining risk behaviour. Staff with longer tenure, those who are less risk tolerant and those with greater seniority are more

likely to report desirable risk-related behaviour (for example, speaking up). Those with high personal risk tolerance are more likely to report undesirable risk related behaviour (for example, ignoring risk consequences of actions). After controlling for personal risk tolerance, gender does not explain behavioural outcomes.

- Staff perceptions of the risk structures (frameworks, training, remuneration systems) are also important for explaining risk behaviour.

How to 'fix' risk culture

Research into risk culture is a new field so little is known about how to change risk culture for the better. What is known has been gleaned from research into safety culture, customer service culture etc. Some suggestions are as follows:

First, make sure that your risk structures (frameworks, systems, policies) are in order. Robust structures are arguably necessary (although not always sufficient) for producing good risk outcomes. ISO 31000 is a great resource for senior leaders to guide best risk practices. Ensure that the risk function is well resourced and that risk training/education is adequate. It is particularly important to ensure that performance measurement and remuneration systems support risk management rather than short-term profits. For example, in firms that have implemented gateway systems whereby staff may not participate in the bonus pool or be promoted unless they have met all their risk management objectives.

Second, targeted intervention may be warranted in the business units where risk culture is significantly less favourable than the industry or company norm. It is possible that key staff such as local managers and opinion leaders are sending mixed (or even negative) messages about the priority of risk management. In some cases staff may have to be replaced. In others staff may need to be coached to provide clearer guidance about the priority of risk management, especially during times when performance is under pressure and staff may be tempted to cut corners. The evidence from research[5] suggests that culture is strongest in business units that have:

- smaller numbers
- greater cohesion between staff
- high social interaction
- interdependent tasks
- high average tenure
- leaders who provide lots of direction (on risk management in this case)
- leaders who behave consistently
- leaders who are transformational.

Further research and culture assessments

Our research into risk culture and misconduct is ongoing. We are looking for industry research partners to be involved in this challenging but exciting endeavour.

Elizabeth Sheedy can be contacted on (02) 9850 7755 or by email at esheedy@mafc.mq.edu.au.

Notes

1 International standards for risk management are detailed in ISO31000. According to ISO 31000, risk management refers to 'coordinated activities to direct and control an organisation with regard to risk' with the aim of ensuring that the firm meets its objectives. It includes a wide range of activities including risk assessment, identification, analysis, evaluation, treatment, monitoring and review, communication and consultation.

2 Sheedy, Griffin and Barbour 'A Framework and Measure for Assessing Risk Climate in Financial Institutions' available at http://link.springer.com/article/10.1007/s10869-015-9424-7?wt_mc=internal.event.1.SEM.ArticleAuthorOnlineFirst

3 For more information see Sheedy and Griffin 'Risk Governance, Structures, Culture and Behaviour in Banks: A View from the Inside' available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529803

4 We measured behaviour in the survey context that is, self-report and observed behaviour of peers.

5 See Ehrhart, Schneider and Macey, 2014, *Organizational Climate and Culture*, Routledge.