

Corporate risk management and the madness of a Prince of Denmark



The Walker review raised the bar and set the expectations on how NEDs should oversight risks in public companies. Sir David Walker said: *"The fundamental change needed is to make the boardroom a more challenging environment than it has often been in the past. This requires non-executives able to devote sufficient time to the role to assess risk and ask tough questions about strategy."*

NEDs cannot be everywhere in the company, and in most cases would not have the expertise to judge all the risks they would encounter. In practice NEDs' view of company risk is first and foremost driven by what they hear from the Executive Directors. That obvious weakness is counterbalanced by company Governance functions, in particular corporate risk management, which give NEDs a view of risks that is superficially both independent and produced by experts. Often this view is supplied through the formal lens of Board meetings or the Audit Committee, although increasingly there is direct interaction between NEDs and risk managers. In addition, the embedding of 'a risk management culture' throughout the organisation will often form the basis of a claim by executives that a business is resilient and shock proof. If true that is hugely reassuring to a NED. Indeed a NED can have no realistic chance of meeting their current responsibility to oversight risks without being able to rely on risk management functions and the risk management culture. Under the emerging regime, that reliance will only become greater.

Is that reliance well placed? If a NED doesn't have a definitive answer to that question then the NED's position is fragile indeed. So what should a NED look for when judging the effectiveness of corporate risk management?

Enter a Prince of Denmark

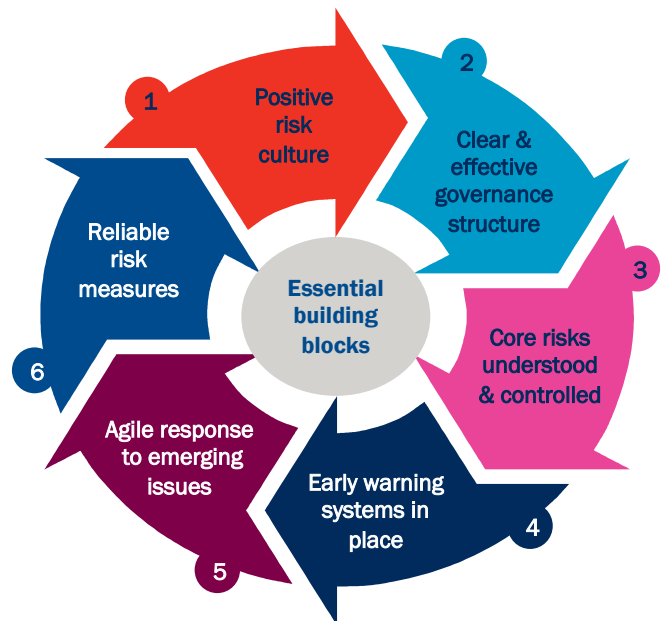
Shakespeare's Hamlet captured the essential challenge risk management exists to address in his great soliloquy:

*"To be, or not to be: that is the question:
 Whether 'tis nobler in the mind to suffer
 The slings and arrows of outrageous fortune,*

*Or to take arms against a sea of troubles,
 And by opposing end them?"*

Since choosing to suffer the slings and arrows is no longer permitted under corporate governance principles, business must take arms and do so as effectively as possible. The mechanisms for this fight are collectively known as risk management, but in fact should be understood as six separate activities, all of which NEDs should expect to see operating to a high standard:

Looking at each in turn:



Culture

Discussions of risk culture, its desirable features and importance to the organisation can generate a laundry list of truisms and clichés which remain frustratingly hard to convert into real actions. In that respect, it is identical to many discussions on the subject of culture, which is by nature a soft

and nebulous concept. Turning this soft subject into something which NEDs can draw confidence from requires discipline.

That includes discipline in the use of language; organisations do not need a risk culture, they need a business culture which treats risk management as a high priority. More importantly, it requires disciplined and real actions which have the effect of reinforcing risk management in the business culture. These actions include:

- Writing objectives to manage risks into the personal objectives of everyone in the organisation. These objectives will vary by seniority and role, from low level staff who must comply with stated procedures through to senior staff that set, review and assess specifically identified risks.
- Linking individual objectives on risk management directly to the reward scheme for computing bonuses and other benefits.
- Providing risk management training to all management levels; training that teaches basic techniques for recognising risk red flags and how these should be evaluated, handled and escalated. Today, interactive web based training modules allow this to be delivered inexpensively and as frequently as required.
- At the executive level, ensuring remuneration schemes do not encourage a cavalier attitude to risk, particularly by offering large rewards for profiting from high risk behaviour and little downside if those same risks produce losses. With the banking crisis, this has become a high profile issue and has already led to a number of guidance papers with the potential that mandatory codes may follow.
- Consistent and repeated messaging on risk management in corporate communications to staff.
- Incorporating risk management disciplines into change activity (such as new systems or product development) in the form of a risk impact assessment that evaluates the consequences to the organisation's risk profile from carrying out a given change.

A final step to establishing a culture that handles risk well is committing senior management time to developing major issue or crisis handling skills. These are needed for the inevitable situation where a risk gets through the defences and strikes the business with an urgent issue.

Management teams operating in a crisis can perform superbly, but they also can degenerate into chaos. An unfortunate fact is that management teams that have had to handle many major incidents are usually very good at managing in those circumstances and muddling through to a resolution. Clearly no NED should be happy with an organisation that is highly accident prone, but they do need to know that when an urgent problem arises the management team are practiced enough to react effectively. The answer is a healthy commitment to urgent issue testing. Devoting three or four days a year to testing simulated issues, developed from scenarios involving real risks the organisation faces,

goes a long way to strengthening the risk culture of the organisation and can identify major weaknesses in the procedures for dealing with particular issues. The NEDs should review the results of these tests as a minimum and they may learn a great deal from attending in person.

Governance

Risk governance is in many ways the easiest risk management concept to grasp. Governance is the combination of policies, delegated authorities, oversight functions and committees by which the Board control what risks the business will take. Policies can be produced, often large numbers of them covering all eventualities, committee structures set up and their terms of reference written. Often a risk appetite statement is endorsed by the Board as the basis for these policies and committees. Unfortunately, whilst the concept is simple, the practical realisation of risk governance often seems unsatisfactory.

Common failings in the way risk governance is implemented include:

- Policy rules are too numerous or complex to be fully understood and applied.
- Some important risks are not well addressed by the policy rules.
- Risk governance does not align to the way the business organises itself and there is uncertainty over who can make management decisions and in what forum.
- Role confusion between those responsible for management and those performing oversight.

Ultimately most of these failings come back to the gap which frequently exists between the control over risks that the Board wants and the actual control that the governance framework provides. Often the gap between the NED attitude to risk and the reality of the governance framework is even more severe as Executive Directors can fall back on their day to day management contacts to gain comfort. A litmus test for risk governance is how many occasions NEDs have been made aware of an issue or a management decision which they feel they should have been informed of earlier or, in the case of the decision, consulted on. Fit for purpose risk governance should virtually eliminate such situations.

Fixing risk governance usually does not rest with devising a high level Board risk appetite statement; these statements rarely help shape the governance framework in a meaningful way. What does work is gaining a detailed understanding of Board, particularly NED, tolerance for individual risks. This is the kind of exercise that can take more than one workshop to complete but it refines a risk specific answer to governance – which risks need policies, which risks can enjoy delegated decision making and which cannot, which risks need hard limits and which need subjective guidance, which risks need to be monitored closely by the Board (and therefore probably by an oversight sub-committee) and so on. These judgements should then be re-visited annually as part of the discussion on corporate strategy, recognising that a change in strategy may change the way risks should be managed.

Core Risks

In many organisations this is the comfort zone, where the vast majority of risk management effort is focused. The risks are familiar ones and the business knows with a lot of confidence where they need to do work to manage them. This core is routinely illustrated in risk maps where familiar risks are described and familiar 'controlling actions' listed. The quality of these maps varies somewhat depending on the sophistication of its authors but this misses the point that these views are fundamentally poor at capturing two vital perspectives – the size of the risk and the threat of the unknown and unexpected. Business needs to accept reality - we are just not good enough at assessing risks for this method to ever be comprehensive and accurate. No one is good enough, it can't be done, and the world (and any one business) is just too complex for us to rely on our traditional view of risks. Risk sizing, be it subjective or statistically based, is deeply flawed as recent events in the financial sector have demonstrated. Mortality risk projections based on centuries of data can probably be defended, few other statistical measures carry enough weight on which to make definitive decisions on those risks which are acceptable and those that are unacceptable. For previously unknown or unexpected risks, if frequently updated, risk maps may do a good job of keeping up with current events, they will rarely predict them.

Flaws in these core risk assessments are not an argument for junking them. The risks they identify are 'perennial' to the organisation and they need to be managed. They include obvious areas where a significant investment in systems and controls is likely to be justified; long term fixes to address perennial risks. The argument here is that management and the risk function need to spend less time on these well understood risks and devote more energy and time to threats which are not well understood - this is achieved by focusing on Early Warning Systems and Issue Response.

Early Warning Systems

For risk management to do an effective job, it needs to dilute its traditional focus on core risks and build real agility into its working methods. This is achieved by getting the right response to issues which emerge in the business which are known, to the extent that some problem is recognised, but the real extent of the threat is not understood. The reason for focusing effort on these issues is the very evident reality that most major issues that damage an organisation don't appear entirely without advance warning signs. In many years of investigating major risk failures there is almost always some smaller issue, of falling standards, apparently minor errors, or just 'noise', concern voiced within the business, which was ignored as unimportant or low priority and which preceded the blow-up. Risk managers need to react to these warning signs with rapid, precise (and small) exploratory reviews to identify root cause of the smaller issues and the potential they hold for severe problems. These reviews dramatically increase the likelihood that risk reporting will be ahead of the blow-up and have the chance to flag the threat. The major challenges are:

- Being networked well enough in the business to hear about the issues when they happen. Disclosure approaches, which range from notifiable event procedures through to anonymous whistle blowing hot lines, are important mechanisms, but these must be supplemented by informal, relationship based information gathering.
- Judging when you have enough information to reach a conclusion on the threat, and then walk away – getting bogged down in insignificant issues will be a major waste of time and expending time to generate action plans on issues without major risk potential will cripple the business.
- Having managers and risk managers who are comfortable jumping into issues with little preparation time, able to multi-task, and savvy enough to see the bigger implications of a small event.

Issue Response

Black Swan theory is much in vogue of late. It is an attractive theory as it deflects much personal blame – “it was a black swan event, no one could have seen it coming.” It is also in danger of being overused. Few events actually meet the criteria that 'no one' saw it coming. For risk management to be as effective as possible, as effective as it needs to be, then risk managers need to be the ones who 'saw it coming' by identifying the threat early. To address these emerging threats that no one is really certain of, the organisation needs to be very good at something many risk functions have long talked about – scanning the horizon for threats (emerging trends in the economy, bad news from other organisations, regulatory or legal strawmen, concerns of contrarian thinkers) and acting early on them, assessing whether they could 'happen here' and how bad it might be. To do this well takes dedicated time, leaving it to managers during their day job will not and has not worked. It requires time spent on reading widely and monitoring events – the great virtue of the internet age is that there are immense quantities of information and viewpoints, insights and analysis on which to draw. Once you know where the best sources are they are easy to tap into and track. This is not a blank cheque on resource, half a FTE equates to a great deal of threat scanning and communication of those threats.

Time is then needed to investigate the potential of these threats to damage your organisation. A rapid initial assessment will usually determine whether more work is needed and the business needs to be prepared to kick off major reviews in some cases to assess how vulnerable their business is to a particular threat.

Do threat scanning well; treat it as a core activity done by your best people and act on the plausible threats they identify, and risk management will have closed off one of its great blindspots.

Risk Measures

The major value of risk measures, or risk reporting, is to present in a meaningful way what risks are being actively run by the business and how large they are. This information, presented to the Board, should be the basis on which the

Board reviews and endorses the risk positions of the organisation on a regular basis. It is inevitably also going to include some risks which are being run which are unacceptable, or at an unacceptable level, in which case the Board will use the report to track progress in closing off the exposure.

Weaknesses in the way risks are sized were mentioned earlier, in particular, this extends to assessing probability, sometimes over estimated, often under estimated. The most realistic and effective approach to risk reporting may be the simplest; one which focuses on the worst case impact of a risk event after having taken credit for the business controls which reduce the size of that loss. The resulting exposure report can combine financial risk metrics (e.g. loss on a loan book in a severe recession scenario) and subjective ones (e.g. reputational damage of a major regulatory breach). Reporting that provides equal prominence to probability, and edges some risks off the radar as a consequence, should be a concern.

Other risk reporting needs to prominently include data on incidents, losses and near misses of whatever size, together with an evaluation of any that could have the potential for larger significance. Reporting of issues from Internal Audit, or compliance monitoring, should also be included as a measure, with resolution performance against these issues. These points of data inform a NED of the level of operational noise in the machine and the responsiveness of the business to resolving issues with its risk control environment.

And will it always work?

No, surprises will still occur. But tackling methodically and with energy all the risk management mechanisms described above will produce dramatically better results than what can be a narrow focus on familiar, core risks. In particular it will produce an organisation that experiences fewer shocks and produces better responses when shocks do get through.

A cautionary note, risk management can be overdone when it leads to a paranoia to take risks and make aggressive business decisions. This is the risk of too much risk management, and was eloquently expressed in the conclusion of Hamlet's great speech:

*"Thus conscience does make cowards of us all;
And thus the native hue of resolution
Is sicklied o'er with the pale cast of thought,
And enterprises of great pith and moment
With this regard their currents turn awry,
And lose the name of action."*

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010

info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD

This risk is a real one, and more organisations are falling victim to it as the prevailing regulatory culture becomes hostile to risk taking. It is a dangerous path when organisations put in additional risk management because they can, know how to and believe more risk management is better risk management. That logic is false and needs to be countered by consistently referring back to the requirements of the NEDs – does the approach being followed really serve their needs? If the link is not obvious and persuasive, then the extra layer of risk management probably shouldn't be applied.

The need for assurance

In practice, observing the business from the remote viewing platform of a seat at the Board is not a particularly effective place to evaluate whether an organisation's risk management is sufficient for a NED to rely upon. The Board often see the professional presentation materials but do not see the dysfunction that might sit behind it. That is why one of the Board's top priorities for assurance should be the effectiveness of corporate risk management. Internal Audit often perform such work but this needs to come with the major caveat that Audit's closest business relationships are usually with risk managers and critical challenges may be tempered as a result. In addition, in many cases, Internal Audit has been (quite rightly) influential in the approach to the risk management which the organisation has adopted and its independence is somewhat compromised. Experience suggests these reviews are best performed by external specialists provided they are committed to understanding the needs of the specific organisation and developing a view of weaknesses which addresses those needs rather than a generic boilerplate.

Kingston Smith Consulting LLP, the business protection consultancy, is ideally placed to help review the effectiveness of risk management as our team blends individuals with deep risk expertise and those who have experience operating on the Boards of large and small businesses alike. This combination results in an approach to assurance that utilises knowledge of the best risk management techniques available, but applies them through the filter of commercial common sense to determine what is appropriate and valuable to the client in each case.