

Risk Management – When Big is not Beautiful



This is a paper in our Non-Executive Director Briefing series.

When attempting to manage risk, big is almost never beautiful. Big risks usually equate to big problems, with lots of effort needed to bring them under control or a high premium to pay for someone to take them off your hands. And big organisations are far from beautiful when it comes to its Directors and Executives fulfilling their duty to effectively manage risk. When a business reaches a certain level of size and complexity it may be impossible for a relatively small number of senior people to really understand and manage the risks they run even when supported by a large infrastructure of helpers.

The Walker Review, the Combined Code review which followed it, and numerous comments from government, quasi-government (e.g. FSA) and pan-national organisations have ventured a solution to this problem based on getting more from the Board – more time, more knowledge of the business and more insight to its risks. There is far from widespread confidence that this will result in improved risk management as the basic challenges of size and complexity may be insurmountable given the lack of tools these senior teams have available to support them. These tools appear, like human abilities, to be effective only up to a certain level of complexity beyond which they (and their operators) cannot cope.

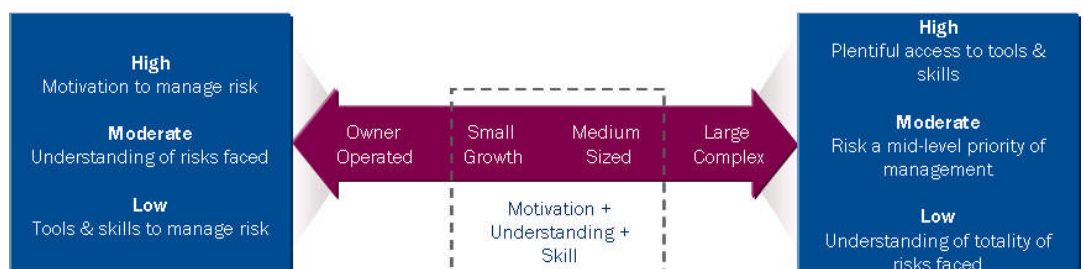
When it comes to effective risk management there is a continuum. It starts with owner operated businesses where the owner is intensely aware of the risks they face and highly motivated to manage them, but probably lacking in tools and skill on how to do that in practice. This continuum extends through to the largest businesses where tools

and skills are available in great quantity but the size of the business has obscured real knowledge of the risks and managing risk is only a mid-level priority for most managers. Every continuum, though, has a mid-point, and on this continuum that point is the small growth companies and medium sized organisations that make up a significant part of most industries.

Defining 'small growth' and 'medium sized' for this purpose is not a question of turnover or staff numbers, it is a measure of relative complexity – organisations that combine a multiplicity of products, markets and operational processes are effectively large when it comes to managing risk. By contrast small growth and medium sized organisations tend to be more focused, operating in a few niches or using the same core operating model across multiple markets.

In these organisations their Directors can achieve a strong practical understanding of the areas of complexity in their business and they have the resources to acquire the tools and skills needed to deliver a highly effective form of risk management. This combination can give these businesses a significant competitive advantage in terms of stability and certainty which will reassure investors and customers alike, an advantage that the largest and smallest players cannot replicate at a reasonable level of cost.

So what does a mid-size player need to do to realise effective risk management?



Essential principles

Governance of risk starts with the Board and senior Executives and encompasses the combination of structure and process through which they extend control over the business and its risks. These structures and processes are essential as they provide a clear line of control from the very top of the organisation to those people in any business that manage risk on a day to day level – the department heads, managers and team heads who every day make operational and commercial decisions. This is commonly termed the risk framework and while these frameworks vary in detail from company to company, there are a number of essential tasks that any competent risk framework must fulfil:

1. Communicate to the wider business what risk levels and key controls the Board and Executive believe must be complied with. This also includes identifying who has the authority to make decisions on taking risks.
2. Provide reliable information and analysis to the Board and Executive on the actual level of risk and related issues in the business which they can use to monitor business risk and order corrective action if they deem it necessary.
3. Provide knowledgeable advice to the Board and Executive on better ways of managing risk, for instance peer group insights, leading practices and practical steps which the Board can take to improve the organisation's management of risk.
4. Provide advice to the Board and Executive on the risk implications of other business decisions they are required to make, such as setting the organisation's high level strategy and the major tactical, operational and financial decisions in support of that strategy.
5. Provide the Board and Executive with *independent* assurance on business risk, covering:
 - Whether the risk reports they are receiving from the business accurately reflect the real exposures, reporting both the right exposures and the right size for those exposures.
 - Whether the risks that exist are under control in a way that ensures that current exposures are not going to change (and deteriorate) rapidly and unexpectedly.
 - In some cases there will be a need to meet specific regulatory requirements for assurance. For instance in FSA rule compliance, or Sarbanes-Oxley compliance there is a requirement for assurance to be performed on defined elements of the risk and control framework.

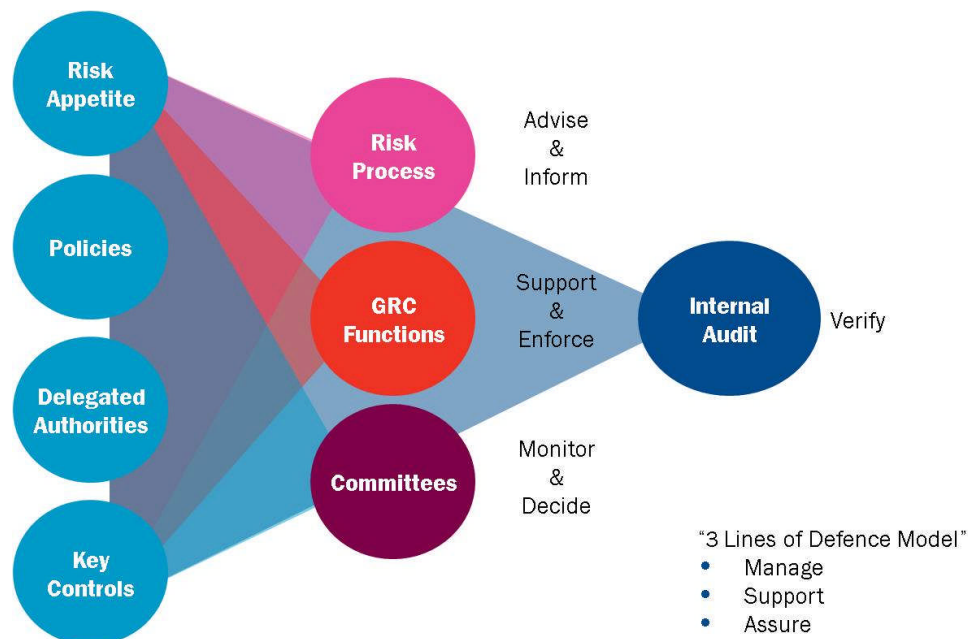
These essential tasks of a risk framework are easy to understand. In the largest organisations the stress their scale places on the risk framework and the linkages it needs to maintain, stretches that framework beyond its breaking point.

By contrast, for small growth and medium sized businesses the risk framework can be made to work. Where it doesn't, even with genuine appetite from the Board to make it work, the problem is likely to be mechanical – the wrong tools and techniques are being used or there is confusion on responsibility for delivering the framework's essential tasks. Often this last issue is a consequence of different departments evolving heavily overlapping responsibilities over time. This obscures the clear risk management purpose they should fulfil leaving gaps, contradictory agendas and inefficiencies (internal audit, risk management and compliance for example).

A structure

Translating the risk framework's essential tasks into practical and effective business activity needs a clear and logical approach. The most common way of achieving this is through an organisational structure usually called the 'Three Lines of Defence' model. This model captures the core tasks of the framework and allocates them between 'Manage', 'Support' and 'Assure' components.

The first line takes the expectations of the Board and Executive on how risks should be managed and communicates these parameters down to a meaningful level which the line managers of the business can apply in a very practical way. The second line supports through production of risk information, provision of advice and guidance and the mechanisms by which the risk decisions of line managers are reviewed, challenged and potentially reversed. The third line is the source of independent assurance that risks are under control and accurately reported.



Looking at each component in turn:

Manage

Risk appetite

The risk appetite is a Board and Executive endorsed view of the level of risk they judge acceptable for the business to take. This is best expressed by individual risk category, e.g. credit risk, market risk, liquidity risk, operational risk. It may be a quantitative value (e.g. a minimum number of days of operating cash on hand) or more subjective (e.g. no new products should

be launched which increase the operational risk of the business). In either scenario, a tolerance is set which can only be exceeded by the business with the approval of the Board. Appetite for risk is, in practice, highly specific to the individual business. The process of discussion by which the Board and Executive develop their risk appetite is a key step by which collective ownership for risk is taken.

Policies

Policies translate risk appetite into rule sets which can be applied by management in the business. In an entrepreneurial business intrusive and numerous policies can be damaging to the culture or be ignored altogether. A well developed risk appetite should clearly identify the areas of risk which the Board and Executive believe to be most critical, risks where they are unwilling to have decisions made without their involvement and where clear parameters are therefore needed – these are the areas where policies should focus. Policy content will include who holds authority to make certain decisions, what steps and information are needed before those decisions can be taken, and what reporting and monitoring is needed on an ongoing basis. For example, a policy on outsourcing business activities might limit approval of outsourcing to business unit heads, require due diligence to have been completed on the third party before approval takes place, and require performance reporting KPIs to be produced after completion in order that the service be properly monitored.

Delegated authorities

Derived from the policies, these document the decision making authority of Executive Directors and cascade these authorities down to lower levels of management. Payment authorisation levels are a simple example; a more complex example is a new product launch where authorisation of several senior managers (front office, back office, marketing, finance, compliance etc) may all be required.

Key controls

Again, in areas of risk where the appetite is for tight control, the key controls managing those risks should be well understood, documented and clearly owned. For instance there is typically a low tolerance for regulatory compliance or legal risk. The operational and management controls that are critical to ensuring breaches are avoided should be well established and given a high management priority. Responsibility for key controls should be added to staff role profiles to provide incentive and accountability.

Support

Risk process

These are the mechanisms by which risks are identified, measured and reported to management and onwards to the Executive and Board. This also includes any risk specialists who may provide advice to management on how best to modify the approach to risk management to work more effectively. These mechanisms must do a good job of capturing all potential risks, determining whether they exist in practice and how severe they might be. This information then needs to be consolidated in a form that provides useable insights to the Board and Executive – a task which is far easier to accomplish in medium sized

organisations where those groups are likely to know and understand the business better than their larger company equivalents. The risk process should also have mechanisms to capture business issues (even those which at first instance appear relatively small), log them, investigate them (to determine their potential to become a major problem) and escalate them.

Head Office functions

Head office functions at the corporate centre play a range of important roles. Often they provide shared service support to business units, and they can play a critical part in delivering business strategy that needs to be co-ordinated across multiple parts of the business. They also should have the remit and capability to play an active role challenging the way business units manage their risks, questioning and escalating issues where they see matters of concern. Central functions such as Finance or Technology provide value by the advice, support and solutions they can provide when issues are observed. They also have an obligation to escalate significant issues to the Board and Executive to push the business to take the right action. There are also often head office functions with explicit responsibilities for risk management and compliance. These specialist functions often ‘run’ (or at least co-ordinate) the risk process and should develop close relationships with the business so they can assess areas where they can add advice and support which helps the business more effectively comply with the rules (those set by an organisation’s policies and / or those set by a regulator). They are also tasked with identifying emerging concerns from outside the organisation that may impact it (e.g. new regulation) and developing a response.

Committees

In the second line of the risk framework, committees perform an oversight and challenge role delegated to them by the Board. They exist to provide more time and focus to particular topics than would be possible at the Board, and to engage with subject matter experts who can provide input and challenge on the subjects discussed. For that reason they are typically more numerous in larger, complex organisations than in smaller, simpler ones. Examples can include the Audit Committee, Credit Committee, Investment Risk Committee, Compliance Committee and Technology Committee. Membership will typically be drawn from within senior management, but should include a Board representative, or at least provide reports of their activity up to the Board.

Critically, they should have amongst their membership individuals who are not responsible for the day to day management of the business activity under scrutiny - individuals capable of challenging that activity. These committees are fundamentally there to oversee the business and are not management meetings, although they often have authority (granted by the Board) to approve a management proposal where that proposal exceeds the manager delegated authority.

Assure

Internal audit

Internal audit forms the third line of defence in the risk framework and performs a direct role in support of the Board and Executive. They are not under the direction of any individual

in the management team; rather their work is authorised and directed by the Board, usually through the Audit Committee where a majority of non-Executive directors are present. Internal audit has the authority to enter any part of the business without restriction and its mandate is to identify whether that business is in reality managing its risks effectively and controls are operating as expected. This is traditionally achieved by performing a series of standalone reviews of different business areas, usually focusing each review on the detail of particular activities and risks. These reviews are particularly effective in identifying control vulnerabilities which form the 'gaps' through which risks could rapidly expand in the future.

In practice internal audit works best when it has a good relationship with management and issues are openly discussed and agreement on a response reached, but ultimately internal audit cannot compromise its independence by, for instance, moderating its reporting of results at the request of management.

Also emerging from the third line must be assurance that the risk assessments the Board and Executive receive from the second line represents an accurate view. This assurance is not achieved from the traditional approach of internal audit and is often missing altogether in many organisations, not least in the banks who have suffered the greatest losses from the recent financial crisis. This problem can be remedied by extending the work of internal audit to provide closer to 'real time' assurance on the size of risk exposures (which will require them to use some different methods); or through the risk management team, although this will probably lead to some role confusion and potential conflict with their 'support and advise' remit.

Where an organisation lacks many of the core components of an effective risk framework defined above, internal audit can act as a temporary alternative as it is able to access the business directly and provide an independent view on risks to the Board that they would not otherwise obtain. In this case, as the governance structure is subsequently developed, the Board

will then be able to scale back the level of internal audit effort as it can rely on other elements of the structure, although internal audit must remain at some level as the final independent check on how the business is managing its risks.

Too big to succeed?

So should big organisations despair of ever effectively managing risk? No, although any answer to the large entity risk management challenge which relies on an expectation that a handful of main Board Directors will become all knowing in all the organisation's risks is doomed to fail. Large entities should instead arrange their risk frameworks so they function as a collection of medium sized organisations. This means managing risk at the level of complexity where the techniques we use for managing risk, and the people who operate them, can still function effectively without being overwhelmed. Risk frameworks operating at a division or country level should have all the elements of a complete framework present including non-executive directors, specific policies and risk reporting, industry specialist risk support teams and dedicated internal audit. In this way these units can achieve most of the advantages of effective risk management that medium sized organisations have. It is a step away from a 'one group' concept, and it is not the leanest possible structure for risk governance of a large organisation. But it makes the task of managing risk something ordinary mortals can accomplish, and for that reason it works.

Kingston Smith Consulting LLP, the business protection consultancy, is ideally placed to help review the effectiveness of risk management and build practical frameworks which organisations can use. Our team blends individuals with deep risk expertise and those who have experience operating on the Board's of large and small organisations alike. This combination results in an approach 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.

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 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