The risks of risk management
Imagine that you are an audit or risk committee member and it’s that time again. The committee agenda reads something like ‘Review of top 12 risks’. Dutifully you and the other committee members run down the list, discussing, asking probing questions, getting updates from management.

You look around the table and everyone seems engaged. But you can’t help feeling the whole thing is something of a waste of time. The trouble is, the same process is used by your other boards, so this must be how it’s done...

Recently described by a leading governance commentator as, “possibly the most important development in risk management practice in recent years”, this paper sets out Halex Consulting’s thinking on risk management. Our aim being to help boards, audit and risk committees see through the fog of traditional risk management approaches and ensure proper focus on what the business is trying to achieve, and what might prevent its achievement.

The symptoms of poor risk management

In many businesses, there is a tendency towards ‘risk listing’, with the primary focus on documenting, assessing and prioritising lists of risks. Sadly, in most cases this approach adds little value, leading to page-turning discussions around the top 10 or 20 risks whilst diverting attention away from the real value of risk management – helping the business deliver its strategy through achieving its objectives.

In the end, the thing risk listing is most successful at is convincing the board and senior management that they are dealing with risk in the same way as other organisations, since this approach is endemic across UK and international businesses.

There are many symptoms of poor risk management but common themes seem to be:

/ A focus on risks, with little or no linkage to desired outcomes, business objectives or strategy
/ Presenting risk categories (e.g. credit risk) as actual risks
/ No measurable improvement in business performance despite a significant investment (money, time and effort) in risk management
/ Risk and control processes that seem to be an end in themselves, being somehow divorced from the routine operation of the business
/ Incremental accretion of ‘key’ controls to the point where every control appears to be ‘key’
/ Risk identification and assessment being done as an annual, or at best a semi-annual, activity with little focus on changes to risk profile
/ A presumption that risk management is a science rather than an art (remember, risk management is about trying to predict the future!)
/ A growing risk bureaucracy keen on ‘professionalising’ risk management

Sound familiar?
A new approach to risk management

Let’s start with the basics. The purpose of risk management is not to manage risks per se. The purpose of risk management is actually to help the business deliver its strategy through focusing on achievement of its strategic business objectives.

Therefore, having clarity of strategic objectives is a pre-requisite for effective risk management. (COSO suggest categories for strategic, operations, reporting and compliance objectives. We would add viability to reflect UK Corporate Governance Code reporting requirements and possibly one or two others.)

Once defined at the highest level, objectives need to be cascaded throughout the organisation. This is no small job, but even if you go no further, you should still see benefits. Creating a hierarchy of objectives in this way ensures that the whole organisation is strategically aligned. Or, in rather plainer English, that everyone is pointed in the same direction.

Moving the focus away from risks and onto business objectives, or key goals, is also more natural and engaging way to consider risks. In effect, it puts risk in the context of reward and focuses senior management and Board attention on the objectives that the organisation is trying to achieve, and what they need to do to increase the certainty of achieving them. It should also lead to a more forward-looking mind set, increased focus on priorities and greater responsiveness to unexpected events.
Risk appetite and conflicting priorities

Fortunately, this approach also helps deal with the knotty problem of risk appetite (an organisation’s willingness to take on risk). If truth be told, many organisations struggle to get to grips with risk appetite in any meaningful way. Even in risk-mature businesses it can remain a largely esoteric concept.

Far better, and more meaningful, is to consider risks in the context of what you, as a business, are trying to achieve. For example, it’s easier to assess whether you are taking on too much risk (or perhaps not enough risk) when you consider those risks in the context of the objective you are trying to achieve. If the objective is very important you might decide that you can’t take any significant residual risks that might undermine its achievement. Therefore, on a cost versus benefit basis, it’s worth spending more money on controls to mitigate the risk.

Using this approach, the organisation defines a framework of strategic objectives covering both the things it choose to do – such as providing financial services, for example – and those things the organisation is obliged to do, such as comply with law and regulation. For each strategic objective, the Board defines how critical each is to the organisation and, similarly, what level of certainty the Board requires in delivering each objective. The more critical the objective, the more certainty is required that it will be achieved – and therefore the less residual risk the organisation can accept in trying to achieve it.

For those objectives where the current level of confidence (i.e. certainty of achievement) is lower than that required, the organisation is in effect running more residual risk than desired – it is above its risk appetite. Consequently, steps should be taken to manage the excess risk (to increase certainty of achievement), revise the objective (to de-risk it) or simply accept the excess risk (with the associated reduction in confidence that the objective will be achieved).

Using this approach to risk appetite provides the Board and senior management with the necessary context to make well-informed risk decisions without having to define a traditional risk appetite statement – which should be a relief for anyone that has either had to write one or, worse still, had to use one.

Incidentally, defining business objectives that can be ranked in order of relative importance can also help businesses think through and manage the challenge of conflicting priorities. For example, (and thinking about recent real-world events), is it more important to boost short-term profits through increased market share or ensure long-term viability and stable profits through compliance with (fuel emissions) regulations?

There will never be a simple answer to the question of competing priorities, but presenting the Board and senior management with objective-based risk information should facilitate a good discussion.
From risk management to performance management

Extending this model further, imagine that the organisation’s business objectives were RAG (red, amber, green) rated for ‘certainty of achievement’ based on the level of residual risk associated with each. If this were done across the organisation, with achievement of subsidiary objectives feeding into the ‘certainty of achievement’ of higher level objectives, then suddenly senior management and the Board has access to forward-looking performance information drawn from across the organisation.

Senior management would no longer need to ‘read the tea leaves’ of financial variance analyses presented in the monthly management pack to decide where to focus resources. The information would be clearly apparent in the RAG-rating of the business’s objectives. It’s likely that senior management would demand this future-looking performance information be provided alongside the financials in every monthly pack. At this point the risk management process becomes a living, breathing part of the business, embedded within day-to-day management processes and contributing to the performance of the business.

Keeping things honest

But how do you know that the performance information produced by your ERM system is reliable given the level of subjectivity required to assess the likely achievement of objectives?

The answer, we suggest, lies in the effectiveness of your Three Lines of Defence model. If first line management understands what it needs to get right, as well as what it needs to avoid going wrong, and can demonstrate that it is achieving these things, then the second and third lines can be positioned to challenge, validate and assure this. In effect, the first line can become the primary source of (non-independent) assurance to senior management and the Audit and Risk committees since it has complete coverage of the entire business.

In this model, the second line Risk Management function becomes increasingly important by:

- providing independent risk assurance – confirming that management’s assessment of risks is fairly stated
- validating first line risk information provided to senior management, the Board and its committees
- giving its own independent opinion of risks (including horizon scanning) and the certainty of achieving strategic business objectives

The third line (Internal Audit) remains responsible for providing independent assurance over all aspects of the organisation’s activities, including looking at the ERM system and the work of the second line. A brave Internal Audit function may even opine on whether management has fairly stated the certainty of it achieving its business objectives.

Internal Audit’s focus is also likely to become more strategic, moving away from a preponderance of detailed process and control testing (since management should have this satisfactorily covered) to one of asking, “What’s been missed?” It should also include consideration of ‘soft controls’ (such as ‘tone at the top’, governance arrangements and risk culture) as well as assessing how management gets assurance over its processes such that it knows the business is ‘under control’.
About Halex Consulting

Founded by Christopher Burt, formerly a partner with one of the UK’s leading governance consultancies, Halex Consulting specialises in providing clear, practical governance strategy, risk management and assurance advice and support to some of the UK and Europe’s leading financial services businesses.

We have seen a wide range of risk management systems and the different types of risk information provided to boards and audit/risk committees – both the good and the bad. This has helped us develop an intimate understanding of what really matters to boards and what organisations need to get right. Using this understanding, we provide clients with bespoke, light-touch consultancy to help them transform the quality and effectiveness of their risk and broader governance arrangements.

If you would like to explore further the ideas and suggestions raised in this paper, or would like more information on how Halex Consulting can help you improve your governance, risk or assurance arrangements, please feel free to get in touch.

Contact

CHRISS BURT
Halex Consulting Limited
86-90 Paul Street / London / EC2A 4NE

+44 (0)7905 469039
+44 (0)20 3823 6569
chris.burt@halex.uk.com

Halex Consulting Limited is registered in England & Wales, company number 6770271, registered office address 86-90 Paul Street, London, EC2A 4NE