Halex
CONSULTING

The risks of risk management

Halex
CONSULTING

The risks of risk management

Imagine you are an audit or risk committee member and it's that time again. The committee agenda says 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...

This paper sets out Halex Consulting's thinking on risk management. We help boards and audit/risk committees see through the fog of traditional risk management approaches and ensure appropriate 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!)

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 achieve its strategic business objectives.

Therefore, having clarity of strategic objectives is a pre-requisite for effective risk management.

We suggest categories for:

- strategic aims
- operational efficiency & resilience
- financial performance & reporting
- conduct & culture
- legal & regulatory compliance
- ESG
- continued viability

Once defined at the highest level, objectives can be cascaded throughout the organisation. Use of cascaded objectives also ensures that the whole organisation is strategically aligned. Or, in rather plainer English, that everyone is pointed in the same direction. This is no small job, but even if you go no further than clearly defining your top-level objectives, you should still see benefits.

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

Moving the focus away from risks and on to business objectives (or key goals) is also a more natural and engaging way to consider risks.

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 is 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 (such as compliance with law & regulation), you might decide that you can't take any significant 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.

Counter-intuitively, the opposite might also be true. For example, you may have an important objective, such as entering a new market, which requires you to take more inherent (gross) risk in order to achieve it – although even in this case it is likely that the organisation will want to minimise residual (net) risk to increase the chances of a successful outcome.

Setting risk appetite by objective (or category of objectives) provides the Board and senior management with the necessary context to make well-informed risk decisions. Standard risk appetite statements don't help with this thinking. Putting risks in the context of what you are trying to achieve does.

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.

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

At this point, you will now have a positively useful enterprise risk management system. But there's more value to be gained.

Imagine that you RAG (red, amber, green) rated your objectives for 'certainty of achievement' based on whether you are managing to get things right, as well as managing your risks. If this is done across the organisation, with achievement of subsidiary objectives feeding into the 'certainty of achievement' of higher-level objectives, then suddenly executive management and the Board has access to forward-looking performance information drawn from across the organisation.

The executive team no longer needs 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 easy to envisage 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 becomes 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
- identifying any new or emerging risks (including horizon scanning) not identified by management
- giving its own independent opinion on 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'.

Why do this?

You probably already have a sinking feeling that this is all rather complex and a lot of work. And to an extent you would be right – risk management transformation is never going to be easy. However, there are a number of 'quick wins' that will have an immediate effect on the way the Board and committees consider risks.

It's likely that implementing key aspects of this model will result in considerable change affecting all aspects of your organisation – including how the Board directs, management manages and the business performs. The benefits, however, are likely to be considerable – including enhanced business performance and strategic alignment, increased employee engagement in the risk process, rationalisation of key controls, simplified risk and control reporting (management and regulatory) and improved Audit / Risk Committee line of sight into the first line. The model also aligns closely with UK Corporate Governance Code risk management requirements (including the viability statement).

About the Author

Chris Burt is an experienced board evaluator, strategy advisor, risk thought-leader and a co-founder of the Risk Coalition.

Chris instigated, chaired and is principal author of the Risk Coalition's 'Raising the Bar – principles-based guidance for board risk committees and risk functions in the UK financial services sector'.

Raising the Bar has since been recognised internationally as leading guidance on the role of the board risk committee and second line risk function.

About Halex Consulting

Halex Consulting has worked with many of the UK and Europe's leading businesses, providing clear, practical governance, risk management and assurance advice and guidance.

We specialise in providing clients with bespoke, light-touch consultancy to help them assess and transform the quality and effectiveness of their:

- Risk governance arrangements
- Board and/or Board Risk Committee
- Risk function and framework
- Internal audit function

Our experience means we understand what really matters to boards and what organisations need to get right.

Please get in touch if you would like to explore further the ideas and suggestions raised in this paper, or would like more information about how Halex Consulting can help you. We're always happy to talk.

Contact

Chris Burt
Halex Consulting Limited

86-90 Paul Street / London / EC2A 4NE

M +44 (0)7905 469039
T +44 (0)20 3823 6569
E 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