Seven Traits of Highly Effective ERM Frameworks

Emma Price, Director Enterprise Risk

Introduction

Recent studies claim that "companies with more mature risk management practices generated the highest growth in revenue, EBITDA and EBITDA/EV"[1] This aligns with what risk practitioners have known for years; that developing an effective, embedded and sustainable enterprise risk framework is vital to supporting business growth and protecting revenue. However, aspiring to more mature risk practices and actually realising them are significantly different, particularly given today's resource and cash-constrained environment. Risk practitioners need to deliver the maximum value possible whilst minimising resource utilisation and, as such, they are looking for quick wins delivering cost efficiencies on the one hand, and business performance improvements on the other. This paper characterises the cardinal traits that risk practitioners should employ if they want to maximise the value of risk management, and considers how efficiencies can be exploited.

The Seven Traits

The seven identified traits of highly effective ERM frameworks are as follows:

1. **Defining, communicating and applying risk appetite to improve decision making.** Explicit focus on risk appetite is a key element to consider when defining the risk framework. Not only does an understanding of the organisation's risk appetite inform decision making, it also enables it to be more agile and move more quickly to manage threats and exploit opportunities. Unless an organisation is able to clearly articulate what its risk appetite and tolerance are, and communicate this so that these concepts and the boundaries involved are fully understood, decisions will be made and actions taken that may involve exposing the organisation to greater levels of risk than it is able to manage. This has the potential to impact the bottom line, and to have significant repercussions in terms of reputational and/ or brand damage. As a result the Board and management's understanding of the risk appetite needs to be 'real time', meaning that as the internal and external environment changes, so too does the understanding of the risk appetite.

   In the UK, the 2010 UK Corporate Governance Code included a provision that *"The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives."*[2] In response to this, the UK Institute of Risk Management recently published a guidance paper on risk appetite and tolerance[3] that helps organisations understand these concepts more clearly, and offers thoughts around how such boundaries can be established. Whilst the process of defining risk appetite may be somewhat complex, the benefits of investing time in this activity are clear. Once the organisation understands how its significant risks should be defined and prioritised, resources can be focused on treatment activities for these risks, and the time, money and people wasted working on the management of less significant risks can be avoided.

2. **Using analytics to understand the full risk picture.** Most organisations understand qualitative risk assessments, however fewer businesses use analytics to understand the deeper risk picture. As the current environment becomes more uncertain, complex and connected, there is a need to leverage the immense amounts of data an organisation generates to effectively inform risk and decision taking. As such, the opportunity to understand detailed aspects of the risk such as risk interdependencies and the financial impact in the context of business strategy and external factors may be missed if the need for quantitative data is ignored. In addition, analytics can help with the identification and management of emerging risks. Many organisations focus only on the short term, using lagging indicators and treating risks as independent events, which does not present an accurate picture of the organisation's true risk exposure. There is therefore a need to consider leading indicators that may give an insight into risks that are 'on the horizon', and to consider how risks interact to give rise to new threats and opportunities. By looking ahead and monitoring trends in the internal and external environment, the organisation is able to prepare and behave proactively when necessary, with better agility and efficiency than its competitors.

3. **Exploiting technology.** Ernst & Young believe that *"Effectively harnessing technology to support risk management is the greatest weakness or opportunity for most organizations"*[4]. Many risk systems are now complex databases that can store and report data. Some however offer analytical as well as management capabilities and are therefore able to identify interdependencies between risks, and provide quantified reports in different formats for different audiences e.g. dashboards for senior management, quick views for the average user, and detailed reports for the risk team. In addition, risk systems can run a variety of modelling programmes such as Monte Carlo analysis, scenario analysis, and stress testing, which are increasingly needed to understand the impact of external events on the organisation. Nascent visual technologies such as interactive risk bow ties, horizon-scanning risk radars and integrated key risk indicators promise to greatly enhance the ability to both describe and control the risk landscape from a position of advantage.

   Furthermore, risk systems can be used to track metrics such as key risk and control indicators which are increasingly being used to monitor performance around risk and control activities. Such metrics are able to provide early warnings as to whether the management actions put in place to address risks are as effective as anticipated, and therefore provide the opportunity for changes to be made before it is too late. Importantly, exploiting the analytical and reporting capabilities of software has a huge impact on time savings, as analysing vast quantities of risk data manually is virtually impossible in any kind of meaningful way. By automating analysis not only is the chance of human error decreased, but the time savings made mean that resources are free to focus on other significant business activities. Whilst the initial time and financial investment in software may seem large, the current economic conditions and competitive software market mean that now more than ever before, ERM solutions are available at competitive prices, and the longer term time and cost savings should easily balance out a cost benefit evaluation. As EY concludes: *"Current GRC tools have the ability to enable an entire risk agenda."*[5]

4. **Defining suitable reporting mechanisms**. An essential element of ERM is the consistent production of good quality, useful information at all levels to inform decision making. This means producing the right information in the right format for the right people at the right time so that informed decisions can be made. In order to achieve this, there needs to be an appropriate supporting risk governance structure that defines how risk data flows around the organisation, what should be escalated, when and to whom. Leading practice organisations specifically focus on reporting high quality, clear risk information, meaning that the messages that need to be delivered are clearly reported and are not hidden by high volumes of spreadsheets, charts and graphs. Additionally, more mature risk organisations also automate risk reporting which not only provides the opportunity to save valuable man-hours, but also allows for a more in-depth analysis of the data which is less likely to be exposed to manual error.

5. **Integrating the risk functions into the business.** A key difference between ERM and more traditional forms of risk management is the approach taken to the operation of the discipline. Traditionally, risk activities take place in silos meaning that there is little to no communication across and between the broader risk functions e.g. 'risk', health and safety, insurance, legal/ compliance, finance, internal audit etc. As a result the board and its committees often receive an unreliable view of risk, with inconsistent messages and even conflicting data. Additionally, the business is bombarded by requests for data from different risk functions which results in 'risk fatigue' and ultimately complete disenchantment with the risk process. Using ERM however, a common language and approach to the management of risk means that there are clearly defined responsibilities across risk functions, and coordinated activities where data is shared and analysed as a holistic picture.

   A further benefit to a more harmonised approach to risk activities is that overlaps and duplications can be identified and removed, whilst any gaps can be addressed. This means that resource redeployment can take place to achieve a more efficient and streamlined approach to risk management. A more integrated approach also has the added benefit of ensuring that the 'risk' function is not an independent body removed from the business with little to no understanding of operational issues. By working across functions and embedding risk management within existing business processes such as strategy setting, internal audit, financial planning, performance management, supply chain and procurement, the risk function is forced to be an integral part of the wider business, and to understand how they can best help the business to manage the risks it faces. Similarly, if the different parts of the business are given the opportunity to participate in the risk framework design, they are more likely to buy-in to the approach, which is also more likely to be adapted to the actual needs of the business.

6. **Appointing a C-level risk executive**. Traditionally found in financial services, more non-financial sector organisations are now utilising this role to drive ERM activities. *"The presence of a CRO or other individual with overall responsibility for risk management is a key indicator of success at building an enterprise-wide risk management process. Besides taking a more proactive approach, the Harvard Business Review Analytic Services study found that organizations with a CRO did more extensive advance planning than other companies in*

almost every major risk area — notably, information security, new regulations, scarcity and/or cost of capital, and the prospect of another asset bubble developing."[6]

The role and responsibilities of the CRO or equivalent may vary between organisations, however the benefits of appointing a CRO include the commercial knowledge and perspective that the CRO brings to the risk function. Involving the CRO in activities such as organisational strategy setting means that the risk approach is aligned to business objectives, and the threats and opportunities involved in meeting strategic objectives can drive the risk programme. By taking a high level and tactical view of risk, the CRO is able to influence investment decisions, and so add real value to the organisation's agenda. In addition, employing a C-level risk executive who has oversight of risk activities across the business, can hold risk based conversations at all levels, and who can sponsor and coordinate the collaboration of disparate risk pursuits means that risk management maintains a highly visible and active position within the organisation.

7. **Addressing risk culture.** Risk culture refers to the behaviours, beliefs and values that individuals within the organisation hold about risk management. The power and importance of the risk culture cannot be underestimated; "*The Risk and Insurance Management Society (RIMS) contends that the financial crisis resulted from a system-wide failure to embrace appropriate enterprise risk management behaviours*"[7]. This may be an extreme example, but organisations that consider and address risk management culture as part of the risk framework are more likely to develop a sustainable and embedded risk approach. This avoids the situation where the same risk management initiatives seem to occur every couple of years as they have been unsuccessful in the past – primarily because they have been driven by process change rather than a consideration of both process and cultural change. In order to avoid wasting resources by repeating the same mistakes, consideration should be given to the required risk behaviours, beliefs and values, and the following steps undertaken:

    - Identification of what expectations the organisation has of individuals regarding risk activities. This should then be communicated clearly.
    - Provision of the necessary support to allow people to meet these expectations e.g. training, tools, resources.
    - Use of appropriate incentives and sanctions to encourage the required behaviour.

    Underpinning all this activity is of course the need for the right 'tone from the top', that is the active demonstration by the Board and senior management of the desired behaviours, beliefs and values associated with risk management; for example demanding risk based meeting agendas and using risk data to inform decision making. The Board needs to plays a leading role in defining the risk culture and promoting a 'no surprises' approach where bad news is quickly escalated and managed in a way that does not allocate blame. In this way, the organisation quickly gains a heightened awareness of the importance of risk management which in turn contributes to a mature risk culture and effective risk management practices.

Applying the Seven Traits in Practice

In an ideal world all seven traits would be implemented effectively within an organisation, however the reality is that various organisational constraints mean that this is not always possible, and ultimately implementing some well is better than all poorly. A highly effective and sustainable ERM framework is not something that can be achieved over night; rather it is the final destination on a journey and as such, is likely to take time and need to be addressed in stages or as projects.

The first four traits discussed in this paper are linked, and therefore make a sensible place to begin an improvement project addressing the ERM framework. Approaching the projects in a coordinated manner will also deliver efficiencies in resource usage. For example, procuring or enhancing a risk software system facilitates the automated production of risk reports, metrics, alerts and analysis in the form of various simulations and graphics. This can be further broken down into two sub-projects: the first to procure or enhance the software; and the second to determine what risk data needs to feed into the system to produce the required analysis, metrics and reports. As more of this information becomes automated, resources are freed up to focus on other key business activities.

Underpinning this data however, is the need for a clearly defined risk appetite which will then drive and determine the information entered into the system, and the level of significance with which the outputs are treated. This is a further project, and the one that should be attended to first.

Addressing the first four traits will provide demonstrable benefits to the organisation in the form of:

- exploiting opportunities and managing threats within the boundaries of the organisation's risk appetite;
- quantified, forward looking data painting a realistic picture of the organisation's risk exposures in sufficient time to manage them proactively;
- saved man-hours and more detailed analysis from automated reporting and analysis; and
- informative, clear risk reports that can be used to underpin strategic business decisions.

Once these benefits are being realised, a strong argument exists to implement the remaining traits which focus on the more time consuming and challenging aspects of organisational and cultural change.

Conclusion

By developing an effective risk framework, organisations have a real opportunity to build value through increased revenues, growth and competitive advantage. Those with existing ERM frameworks have the opportunity to improve these or develop them further in line with the traits listed above. Those with more traditional risk management processes in place, have an unprecedented chance to move towards a more proactive risk management approach, and adopt leading practice traits as part of this process. As EY states: *"Risk is now becoming the fourth dimension of business. People were the first dimension. Process became the second dimension during the height of the manufacturing era. Evolving technology formed the third dimension. Embedding risk as the fourth dimension of business has the potential to fundamentally transform how organizations connect risk to reward."*[8]

Footnotes

[1] Ernst & Young, Turning Risk into Results. 2012, p4

[2] Financial Reporting Council, The UK Corporate Governance Code. 2010, p19

[3] Institute of Risk Management, Risk Appetite & Tolerance Guidance Paper. 2011

[4] Ernst & Young, Turning Risk into Results. 2012, p3

[5] Ernst & Young, Turning Risk into Results. 2012, p12

[6] Harvard Business Review Analytic Services, Risk Management in a Time of Global Uncertainty. 2012, p2

[7] RIMS, A Wake-up Call for Enterprise Risk Management. 2009, p4

[8] Ernst & Young, Turning Risk into Results. 2012, p13