ENTERPRISE-WIDE MANAGEMENT OF RISK IS BECOMING AN ESSENTIAL PART OF TODAY'S BUSINESS. **MALCOLM STOKES** OF ZURICH FINANCIAL SERVICES EXPLAINS THE FINER ELEMENTS.

REAPING BENEFITS FROM RISK

Corporate risk management is undergoing dramatic fundamental and far-reaching change. Its centre of gravity is moving from treasury and insurance departments towards line management and the boardroom, as a much broader enterprise-wide perspective on risk is adopted. The focus is shifting from operational hazards and pure financial risks to a much more strategic view of threats to business success and an appetite for upside risk.

The increasing demands of regulators and stakeholders is adding to this momentum, as enterprise-wide risk management (ERM) becomes an essential element of modern business. However, the degree to which companies integrate risk management into their everyday business and culture differs widely. For some, it is merely a matter of compliance, yet for others it is a sophisticated response to the challenges of a fast-changing business world.

The fact that some companies are taking risk management well beyond minimum compliance implies there are competitive advantages to be gained from doing so. In this article, we take a broad look at ERM, the commitments involved in implementing it effectively, and the benefits businesses can achieve as a result.

WHAT IS ERM? ERM is a powerful management tool that gives senior executives a full understanding of their key strategic and operational risks, and therefore a sound basis for making decisions.

As its name suggests, the objective of ERM is to manage risk as an integral part of enterprise management across all functional, operational, and cultural boundaries. It also means recognising that business risk has a positive aspect, an upside linked to opportunity, which needs to be managed proactively.

ERM treats risk as the uncertainty around achievement of corporate objectives. Risks, in this sense, can be threats to, or vulnerabilities of, the existing business and its future opportunities. Looked at in this way, business risk management becomes a source of competitive advantage that informs strategic decision-making. An effectively implemented ERM process will usually include:

- a systematic approach to risk identification;
- a common language for describing risks;
- a consistent reporting framework;
- prioritisation of risks for allocation of resources;
- recognition of opportunities to offset or pool risks in a portfolio;
- a disciplined and structured approach to risk appetite;
- sharing of risk information across traditional silos; and
- open risk communication with stakeholders.

> 'BY FOCUSING ON THE ONGOING MANAGEMENT OF RISK AT ALL LEVELS AND ACROSS ALL FUNCTIONS, ERM IS A POWERFUL METHOD OF CONTROLLING RISK'

MOVING TOWARDS ERM. Most companies have already established processes to manage risk. However, as shown in *Figure 1*, the focus of these processes and the value they achieve depend on how much commitment a company makes to risk management, and how far it moves on the journey towards full ERM.

Historically, risk management has been the remit of the insurance and internal audit functions, with a rather narrow focus on hazard and operational risks. The process expanded, particularly in the banking sector, to include quantifying and mitigating financial risks, and therefore it came to involve treasury departments. ERM takes risk management a stage further, adding the upside of risk and moving it closer to where business decisions are taken. By combining this with a more holistic top-down approach to risk strategy and appetite, companies can focus their attention on the more significant threats to business objectives and achieve even greater value from risk management.

FIGURE 1

The ERM journey

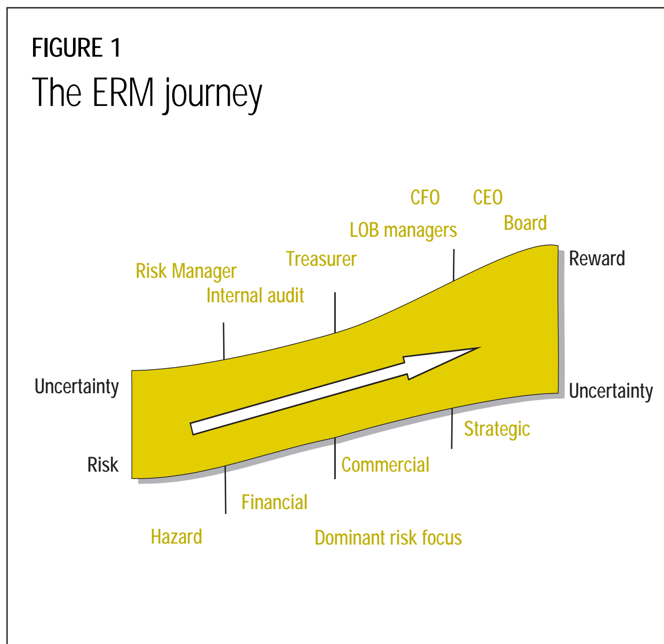
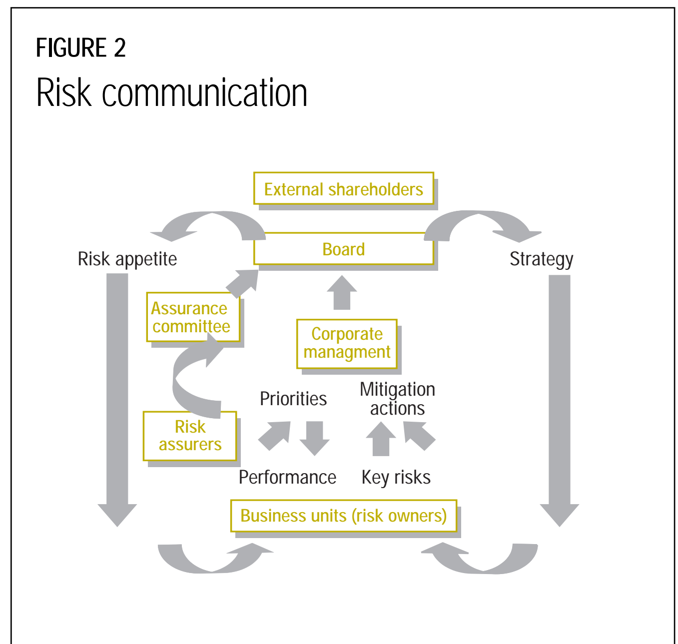


FIGURE 2

Risk communication



'A WELL-DEFINED AND EFFECTIVELY COMMUNICATED RISK APPETITE ENSURES THAT MANAGERS ARE CLEAR ON THE LEVEL OF TOLERABLE RISK AND THAT, WITHIN THESE LIMITS, ANY OPPORTUNITIES ARE EXPLOITED'

CORPORATE GOVERNANCE AS A CATALYST FOR ERM. Directives on corporate governance, the system by which companies are directed and controlled, have plenty to say on the subject of risk management. Although not explicitly requiring companies to introduce ERM, they have certainly been a catalyst for its development.

Regulation aims to safeguard shareholders' investments in companies' assets, including intangibles such as intellectual property and reputation. Guidance such as the Turnbull Report has led to some companies taking further steps to expand on compliance through ERM. Both the Turnbull and more recent Higgs reports on corporate governance have been widely acknowledged for their practical guidance that avoids being too prescriptive – as such, they take a different tack to developments seen in the US, where legislation such as the Sarbanes-Oxley Act is being used to enforce governance principles. ERM is exactly what Turnbull and others recommend: the internal control of risk being embedded in company operations and corporate culture.

But embedding a process is more difficult than simply installing one, because it needs to recognise and work continuously as part of the business's culture and existing management processes and systems. When attempting to control risk, the focus should be on significant threats to fulfilment of business objectives. Note that the operative word here is 'control' and not 'reduction', and that ERM must incorporate mechanisms to both filter and escalate risks to ensure the right risks come to the attention of the board.

Managing risks does not necessarily involve eliminating or transferring them – this depends on their potential upsides and the business's appetite for risk. Furthermore, risk management should be a continuous process – the business environment changes too fast to rely on annual reviews. By focusing on the ongoing management of risk at all levels and across all functions, ERM is a powerful and efficient method of controlling risk.

ENSURING THERE ARE NO SURPRISES. In its 1999 report, *No Surprises*, the Institute of Chartered Accountants of England and Wales argued that incorporating risk information in the annual report should help investors understand the risk profile of companies and, ultimately, help those same companies obtain capital at the lowest possible cost.

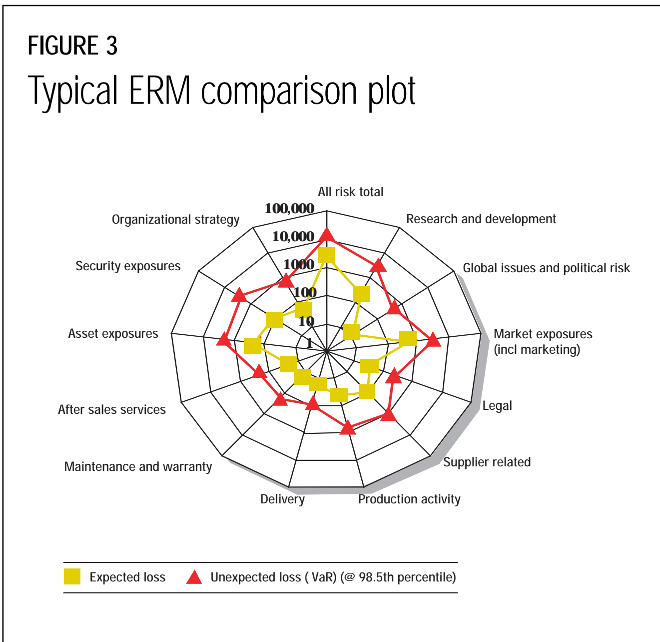
Within the context of risk management, a 'surprise' is an event with extreme risk consequences, which shows a significant deviation from expectations. Because expectations come from assessment of the business environment and from management information, deviations imply poor-quality information, poor judgement in decision-making, gross human error, deliberate overriding of controls or unforeseen events.

Analysts and investors react to deviations, and their judgement will be tempered by their level of confidence in the underlying quality of corporate governance: was it bad luck or bad management? Effective communication, as part of a 'no surprises' culture, can be invaluable in boosting investor confidence. Embedding a 'no surprises' culture means:

- achieving management buy-in at all levels;
- establishing a clear risk management policy and internal control strategy;
- consulting widely and keeping risk management systems simple;
- removing barriers to open communication and cross-functional interaction; and
- getting everyone working together, understanding the risks and acting appropriately.

FIGURE 3

Typical ERM comparison plot



It is clear that a 'no surprises' culture requires the same foundations as an effective ERM process; the two go hand in hand. Having invested the time and resources required to implement a rigorous and embedded risk management system, it is only by communicating this fact that a company can reap the rewards among analysts and investors.

As *Figure 2* shows, risk communication starts with the board, which must:

- Ensure that the business strategy and the risks inherent in it – that is, the business's risk appetite – are communicated consistently to stakeholders.
- Ensure that all stakeholders are made aware of the level of risk which exists within the business and how the business is controlling it. Because of its wide accessibility, this is usually achieved through the annual report and accounts.

QUANTIFYING RISK AND RISK APPETITE. To be successful, businesses must take risks. Therefore, defining corporate risk appetite is an important aspect of an organisation's communications, both internally and externally. A well-defined and effectively communicated risk appetite ensures that managers are clear on the level of tolerable risk and that, within these limits, any opportunities are exploited. In this way, risk appetite will influence strategy and objectives at board level and in day-to-day decision-making throughout the business.

Treasurers will be familiar with the concept of quantifying and mitigating financial risks. Risk appetite means going a step further by considering the whole business as a portfolio of quantified risks and opportunities that can be objectively measured against the risk appetite. Any risks above the tolerable limit will need to be transferred or managed out of the business, with the bigger risks being given the highest priority and largest allocation of resources.

Corporate governance bodies, investment fund managers, credit rating agencies, employees, customers, suppliers and other external groups are putting increasing pressure on companies to be more open about the way they do business. Establishing and communicating the business's risk appetite is entirely in keeping with this drive for more transparency.

MAKING THE MOST OF ERM OPPORTUNITIES. Some businesses adopt a minimal approach to implementing ERM, hoping to avoid too much organisational change. In doing so, their departmental structures can become barriers to progress and they may miss out on important opportunities. Although the in-depth knowledge of specific risks will always come from experts inside the business, independent consultants can help to embed ERM processes in a variety of ways. Through their external perspective they can:

- challenge assumptions and current processes, and act as catalysts for change;
- facilitate pilot risk analyses and in-house training of staff;
- introduce fresh ideas for refining existing processes;
- audit the process to ensure its efficiency and effectiveness; and
- benchmark processes and results against the organisation's peer groups.

ERM takes companies beyond regulatory compliance and creates a business culture environment that can deliver real competitive advantages. Not surprisingly, it is spreading from large and leading enterprises to smaller ones.

However, as ERM becomes more widespread, its original meaning and purpose are inevitably being diluted. All too often companies try to implement ERM using limited resources, without enough understanding and commitment from the top, and with too little education of line managers. As a result, many of the opportunities and benefits of ERM are being missed. To take full advantage of ERM, companies must recognise that it can take them far beyond mere compliance with good governance practice. ERM is as much about maximising the upside as it is about reducing risk.

THE REWARDS OF ERM. There is plenty to gain from implementing an effective ERM system. Some of the advantages include:

- Providing management with a full understanding of their key strategic and operational risks, helping to ensure that objectives are achieved.
- The ability to make faster decisions about the risk and reward of new opportunities and projects, informed by risk awareness and established risk appetite.
- A more easily achieved balance between control and empowerment, allowing entrepreneurial activity to flourish within defined boundaries.
- Helping define and communicate the organisation's appetite for risk, ensuring that the managers take tolerable risks and exploit opportunities.
- Higher credit ratings, leading to lower cost of capital.
- Stakeholders who are more confident that risks are understood and actively managed.
- Greater trust and enhanced reputation, leading to business growth.

Malcolm Stokes is Head of Strategic Risk Consulting at Zurich Financial Services.
malcolm.stokes@zurich.com
www.zurichstrategicrisk.com