

Enterprise Risk Management: Its Origins and Conceptual Foundation*

by Gerry Dickinson**

1. Introduction

Since the mid-1990s, enterprise risk management has emerged as a concept and as a management function within corporations. Enterprise risk management is a systematic and integrated approach to the management of the total risks that a company faces. Its emergence can be traced to two main causes.

First, following a number of high-profile company failures and preventable large losses, the scope of corporate governance has widened to embrace the risks that a company takes. Directors are now increasingly required to report on their internal risk control systems. This is either through voluntary codes, such as the Turnbull Guidelines in the U.K., or by legislation, as in Germany through the “Control and Transparency in Entities” Law.

Second, shareholder value models are playing a greater role in strategic planning. Early strategic planning models paid insufficient attention to risk. Modern strategic planning models are based more on shareholder value concepts, which draw their inspiration from the finance theory where risk has always played a central role.

2. Origins of risk management

Risk management as a formal part of the decision-making processes within companies is traceable to the late 1940s and early 1950s. There were two earlier strands of risk management practice that have more recently been integrated under the broader concept of enterprise risk management. One of these strands relates to the management of insurance risks and financial risks.

For many years, companies have been able to transfer certain types of risks to insurance companies. These transferred risks related to natural catastrophes, accidents, human error or fraud, but as the scope of insurance markets expanded, some types of commercial risks could be transferred, such as credit risks. The existence of these insurance markets forced managers to consider alternatives to the purchase of insurance. Some of these insurable risks could be prevented, or their impact reduced, through efficient loss-prevention and control systems, and some could be retained and financed within the company. This led to a broader approach to the management of insurable risks.

* This paper is an expanded version of an article published on 13 November 2000, by the *Financial Times* newspaper in its series on Mastering Management.

** Professor, City University Business School, London.

In the 1970s, companies began to look more closely at how they managed various financial risks, such as movements in exchange rates, commodity prices, interest rates and stock prices. Financial risk management began, as a formal system, at the same time as the development of financial derivative products, for example, financial futures, options and swaps.

This was no coincidence, since investment banks had developed these financial instruments and their associated markets in part to allow their corporate customers to hedge these financial risks. Hence, financial risk management emerged in much the same way as insurance risk management had previously. It was stimulated by the existence of these financial products, which caused management to consider how much of the risks should be retained within the company and how much should be offset through these external arrangements. The existence of financial derivatives also forced companies to consider more carefully the pricing of risks, how risks could be financed internally, and the value of the additional services supplied by investment banks.

Companies also recognized that insurable risks and financial risks should be managed together, since the purchase of insurance and the purchase of derivatives to hedge financial risks performed essentially the same role. This recognition has led more recently to the development of new risk transfer products that combine both types of risk. One of the early examples of this more integrated approach was the decision taken by Honeywell in 1997 to take out a multi-year contract that combined insurances to cover its property and liability risks and options to hedge the adverse effects of currency movements on the reported profits from its overseas operations.

The second strand in the development of a more holistic approach to risk management arose from more general management thinking. Contingency planning had been a part of corporate policy for many years, its purpose being to identify those activities that might be threatened by adverse events and to have systems in place to cope with these events. Business continuation management extended the practice of contingency planning by requiring more comprehensive internal systems. The corporate responses to the Y2K threat provide a recent example of business continuation management in action. Both contingency planning and business continuation management approaches, however, were limited, since they presupposed that strategic choices had already been made and their role was confined to the effective implementation of these strategies.

3. Defining enterprise risk

Enterprise risk is the extent to which the outcomes from the corporate strategy of a company may differ from those specified in its corporate objectives, or the extent to which they fail to meet these objectives (using a “downside risk” measure). The strategy selected to achieve these corporate objectives embodies a certain risk profile, which arises from the various factors that might impact on the activities, processes and resources chosen to implement the strategy (see Figure 1).

A range of external and internal factors can cause the outcomes of a company’s activities to depart from those set down in its corporate objectives. Some external factors relate to those in the marketplace in which a company competes, such as new entrants into the market, changing consumer tastes or new product developments. Other external factors arise from a wider context, such as changes in the economy, changes in capital and financial market conditions, and changes in the political, legal, technological, demographic and other environments. Most of these are beyond the control of management, although active

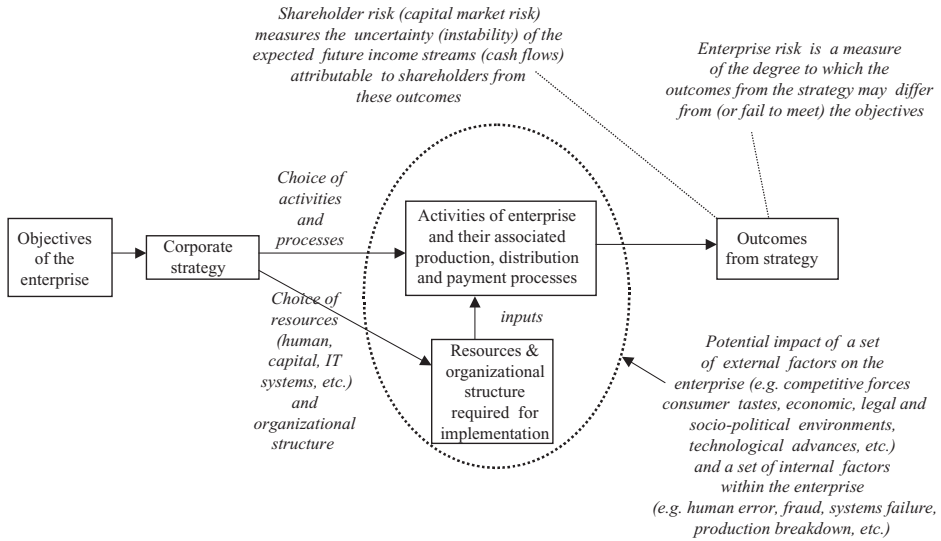


Figure 1: Measuring enterprise risk

enterprise risk management requires that there are systems in place to make a company more resilient and adaptable to major changes. Risk management is a dynamic process.

Another set of factors that can cause outcomes to differ from those planned arise from within the company itself. These are human error, fraud, systems failure, the disruption of production, and so on. These internal causes represent a major part of what are generally known as “operational risks”.

In seeking to assess the impact of the plethora of external and internal factors on the activities of a company, there must be some simplification to make the task manageable, even with the assistance of computer modelling. Increasingly, scenario analysis is being used to measure and manage enterprise risk, with support from management consultancy firms or specialist risk management consultants.

If one measures enterprise risk in terms of corporate objectives, one has a consistent framework of analysis. But there are shareholder value models to consider. Shareholder value models specify that the corporate objectives of a company should be coincident with those of shareholders. However, shareholder risk can only be determined indirectly, since it depends on how the stock market values the expected riskiness (volatility) of the future corporate income streams from the company’s activities. When the corporate objectives of a company are fully aligned with those of shareholders, enterprise risk will be close to, if not the same as, the risk perceived in the stock market. But it should be kept in mind that in both competitive product markets and in risk-averse stock markets, a corporate strategy with a higher risk profile will tend to have higher rewards: there is a compensation for the lack of predictability.

4. Retaining and transferring risk

Since the overall risks of an enterprise are an integral part of its corporate strategy, one way of managing these risks is through the choice of the corporate strategy itself. If senior

managers consider the risk profile of a particular strategy to be too high, they can change the strategy to one with a lower risk profile. Hence, enterprise risk management must be a top-down process.

Just as other corporate decision-making processes take place in a hierarchical structure, so do risk management decisions. The questions of whether to buy insurance or to hedge financial risks depend on the strategic decisions that have already been made. For example, the currency risks of a company arise *because* it has international activities. Thus, if a company's production is located in a country with a strong currency relative to those countries it wishes to export to, one way of managing these currency risks is by relocating its production facilities.

Most of the risks that a company faces cannot be insured or hedged, and so they must be retained and financed internally. Other mechanisms also exist for reducing risk, apart from the purchase of insurance and hedging with financial derivatives. Legal mechanisms can be used, for example. Some risks from commercial activities can be restricted through the use of corporate vehicles, using their limited liability status. Large-scale projects and major real-estate developments are often structured this way: the Alyeska Pipeline Service Company was formed in 1970 to build and service the Alaska oil pipeline; and the Olympia & York Canary Wharf Company was formed in 1985 to redevelop part of the Docklands area in London as an office and residential complex.

Divestment of corporate activities and the outsourcing of operating functions provide other mechanisms for risk transfer. But unlike insurance, hedging or legal mechanisms, divestment or outsourcing represent a transfer of a commercial activity itself, and not just the risks embedded in these activities.

Decisions on how much insurance is bought, how much of the financial risks is hedged, or the degree of divestment and outsourcing that takes place will be largely determined by a few key considerations. The scale of potential loss or, more precisely, the greater the potential adverse impact on the attainment of corporate objectives, the greater will be managers' preference for risk transfer rather than risk retention. Decisions on the balance between risk retention and risk transfer will be not only related to their scale of impact. The degree of information and competence that the company possesses in managing a specific set of risks is also important.

When a company divests or outsources an operation, it does so usually because it considers the recipient to be better equipped and more knowledgeable in managing these activities. For example, the outsourcing of computer and information systems to a specialist organization can reduce the risks of technological obsolescence and systems failure, as well as increasing cost-effectiveness. More knowledge and a greater core competence usually mean lower risk, since the impact of a risk event often depends on who is managing or controlling the underlying process. Similarly, in buying insurance or derivative contracts to hedge financial risks, information about the risk is also important. Companies will tend to have less information on the underlying probability distributions needed to price insurance risks than insurance companies, especially if the insurable events occur only infrequently. This also applies to the pricing of financial risks.

5. Some general propositions on enterprise risk management

This broader concept of enterprise risk management also gives a clearer positioning on how insurable risks and treasury or financial risks should be viewed within the organization. Insurable risks and financial risks are both sub-sets of enterprise risk. Hence, if there were no

insurance markets and no derivative markets or other hedging mechanisms, all the risks that an organization faces would be enterprise risks, since they arise as a consequence of the activities that it undertakes.

We can summarize the above and our earlier discussion on enterprise risk in the following propositions:

1. Enterprise risk is embodied within the corporate strategy of an enterprise (i.e. its choice of corporate activities and its choice of the resources and organizational structure to implement these activities) within the context of the uncertain environments in which it operates.
2. Enterprise risk can only be effectively measured in terms of an enterprise's corporate objectives. The degree of risk is the extent to which the actual outcomes from the activities of an enterprise differ from (a variance concept of risk), or fail to meet, these corporate objectives (a "downside" concept of risk).
3. Where the enterprise is a quoted company, the more closely aligned are the corporate objectives that are set by management to those of its shareholders' interests, the closer will enterprise risk be to the stock market's own risk assessment of the company.
4. Since the financing of the risks faced by an enterprise should be integrated into the overall financing of the enterprise itself, insurance buying and self-insurance decisions and hedging policies need to be closely co-ordinated with its broader cash management and capital structure decisions.
5. Risk retention decisions on insurable risks (e.g. choice of deductible levels) and risk retention decisions for financial risks (e.g. choice of "strike prices" on option contracts) should be determined jointly; both types of risk are subsets of the overall enterprise risk and hence are unlikely to be independent of each other.

6. Organizational issues

Finally, some key organizational issues should be outlined. Since enterprise risk management must be a top-down process, the chief executive and the senior executive team must determine the parameters for the policies and the organizational structure for its effective implementation. Information must be fed back from those closest to the sources of risk, so that senior managers are well informed when formulating their overall risk policy. In addition, management must delegate some responsibility to those closest to where the risks are likely to impact or arise, so that early action can be taken to prevent a small problem growing into a larger one.

Because of the complexity of identifying, controlling and managing risks across a company, dedicated and specialist expertise is required. A new co-ordinating management role is now emerging – that of the chief risk officer (CRO). The chief risk officer, who is usually a senior executive and part of the top strategic planning team, may retain a more traditional job title, such as Group Risk Director, even if his or her responsibilities have now widened, but the title, Chief Risk Officer, is growing in use. Ford Motors, Duke Energy, Koch Industries, Charles Schwab, Fidelity and Royal Bank of Canada have, among others, all appointed such officers.

In addition, the CRO must maintain close links with the chief financial officer (CFO). The financing of risks, whether retained or transferred, rests with the chief financial officer, who will inevitably be a senior executive and will also sit on the main strategic planning committee. The chief financial officer is responsible not only for the purchase of insurance

and derivatives, since these decisions fall within the corporate treasury function, but also for the overall financial policy of the company, which includes the financing of all retained risks.

Corporate governance concerns now encourage boards of directors to develop more clearly defined risk audit functions, including an overview of their top management teams. This high-level risk audit function is often an additional responsibility for the audit committee of the board of directors. Since executive directors themselves have to be monitored, a non-executive director chairs the audit committee in order to give it the necessary degree of independence. The board of directors has the ultimate responsibility for the enterprise risk of the company, being accountable to shareholders and other stakeholders. In countries that have a tradition of having a two-board structure, an executive board and a supervisory board, the chief risk officer should report to the supervisory board. The structure of reporting, risk policy guidelines and information flows for an efficient organization is depicted in the Figure 2.

In financial services companies, such as banks, insurance companies and securities firms, the role of chief risk officer will assume an additional dimension over time. The CRO will most likely be given the overall responsibility for liaising with the government supervisory authority charged with implementing prudential regulations. This additional responsibility is likely to increase under a regulatory environment, which appears to be emerging, where some of the risk monitoring traditionally carried out by a government supervisory authority is delegated to the financial services company itself (see Basel Committee, 2001; Davies, 2001; and Ross, 2001).

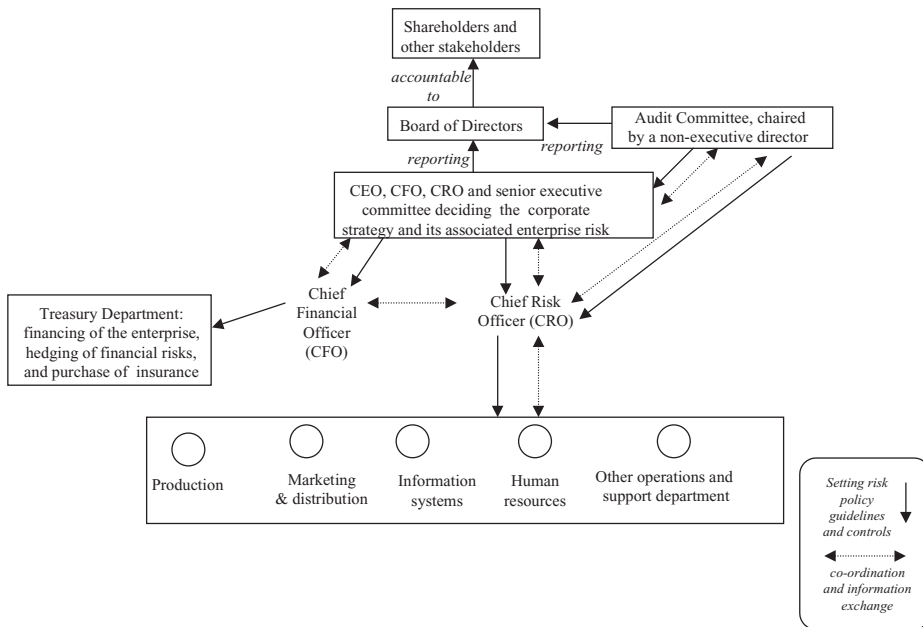


Figure 2: Enterprise risk management and its organizational setting

Conclusion

Enterprise risk management will continue to strengthen its role within the strategic planning process. Since it has become part of the corporate governance agenda, and because boards of directors and senior managers are now more directly accountable for the risks that the company takes, it will likely receive ample financial resources for it to develop fully. Finally, enterprise risk management also provides a coherent framework within which the insurance and financial risks that the firm faces can be evaluated and managed.

REFERENCES

- BANK OF INTERNATIONAL SETTLEMENTS, 2001, *Proposal for a New Basel Capital Accord*. Basel: Bank of International Settlements, January.
- DAVIES, H., 2001, Keynote Address, Insurance Institute of London, London: Financial Services Authority, 9 March.
- DICKINSON, G.M., 1997, "Integrating Insurance and Hedging into the Overall Risk Management of the Firm", *Singapore International Insurance and Actuarial Journal*, Inaugural Issue, Vol.1, August, pp. 161–173.
- DICKINSON, G.M., 2000, "Risk Role Grows to Enterprise Scale", *Mastering Management, Part 7, Financial Times*, London, 13 November, Supplement, pp. 14–15.
- DELOACH, J., 2000, *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity*. London: FT-Prentice Hall.
- DOHERTY, N.A., 2000, *Integrating Risk Management: Techniques and Strategies for Managing Corporate Risk*. New York: McGraw Hill.
- GIAIRINI, O. and STAHEL, W.R., 1993, *Limits to Certainty*, 2nd edn. New York: Kluwer Academic Publishing.
- GRANT, R.M., 1998, *Contemporary Strategic Analysis*, 3rd edn. Oxford: Blackwell Publishers.
- KESSLER, D., 2001, "Anticipating and Managing Risks in the 21st Century", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 26, No. 1, January, pp. 1–7.
- KLOMAN, H.F., 1992, "Rethinking Risk Management", *Geneva Papers on Risk and Insurance – Issues and Practice*, No. 64, July, pp. 3–15.
- LAM, J., 1999, "Enterprise-Wide Risk Management and the Role of the Chief Risk Officer", *Ivey Business Quarterly*, Issue 3, pp.10–18.
- ROSS, S.A., 2001, "Financial Regulation in the New Millennium", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 26, No. 1, January, pp. 8–16.
- ZECH, J., 2001, "Rethinking Risk Management: The Combination of Financial and Industrial Risk", *The Geneva Papers on Risk and Insurance – Issues and Practice*, Vol. 26, No. 1, January, pp. 71–82.