J O I N T C E N T E R
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

The End of Enterprise Risk Management

David Martin and Michael Power*

Related Publication 07-22

August 2007

* David Martin is chief risk officer at AllianceBernstein Inc; Michael Power is Professor of Accounting at the London School of Economics and Political Science. We are grateful for the helpful comments of Greg Connor.

Executive Summary

Enterprise risk management (ERM) has grown in significance since the mid-1990s to become a key resource in the conceptualization and design of risk management systems. We argue that this emphasis is misplaced and contributes to the problem of a divide between analysis and action. ERM may be relevant for regulators and others in need of proof of good governance, but its formulations have become progressively detached from the reality of modern financial organizations. We argue that buy-side risk management practices provide an alternative conception of risk management which is more grounded in operations and which avoids the problems of actionability created by controls-based ERM.

The End of Enterprise Risk Management

David Martin and Michael Power

1. Introduction

The future of risk management has been imagined as a technocratic ideal in which a person sits in front of a multiple computer screens with their hands slowly moving the dials as the risk information flows through the system. The prevailing image is that of mission control at NASA, the control room at a nuclear power plant or a trader in a Wall Street dealing room. On this view, the holism of risk management demands an information infrastructure capable of processing all the risks which impact on organizational strategy. The ideal is also that such systems in financial organizations monitor, validate, protect and adjust levels of capital 'adequate' to the risks of the business.

This image reflects an ultimate hope that risks can in fact be managed in holistic way on an enterprise wide basis, with a strong presence at the center of the organization, often called the Risk Management Division of the Enterprise Risk Management (ERM) function. In support of this aspiration, a number of generic standards and guidelines have been published by a wide variety of bodies which frame risk management as an organizational process (Power, 2007).

Out of these ideas and aspirations, so-called 'enterprise' risk management systems (ERM) began to be developed from the early 90s onwards. One example is a program which was used at Citibank known as Windows on Risk[1]. The Windows, as they were called, were summary views of discreet risk categories that were extracted from independent but highly developed underlying risk management systems that could be used to drill down to the transaction level detail. The innovation of Windows on the risk process was the use of scenarios to evaluate multiple risks simultaneously and then to mandate specific action plans. However, the path of development of ERM has taken it in a somewhat different direction from these first steps. Today ERM has been fashioned with a predominant analytical emphasis on the summary top-level, enterprise view without the orientation towards action of these early efforts.

We argue here that ERM in its various manifestations is susceptible to misplaced emphasis and various pitfalls. In essence, if ERM is to be implemented in a way which helps an entity get to where it wants to go, it needs to have a bias toward action which many applications

[1] One of the authors, Martin, was involved in the development of this program as a risk manager at Citibank.

currently lack. Existing top-down designs for ERM have an obvious attraction for regulators seeking to make senior management accountable, but such approaches are neither realistic nor pragmatic; they are not grounded in the demand for management action, which is always somehow 'outside' the framework. Even supporters of ERM admit that organizations find it easier to populate risk maps than to populate action columns on spreadsheets.

Critical influences on the shape of ERM during the 1990s have come from major regulatory programs, particularly the significance accorded to internal control environments under pillar 2 of Basel 2 and the ICA regime for insurers in the United Kingdom. These and other regulatory systems understandably looked to existing controls-based frameworks as benchmarks of good practice. In particular, in the United States, the design developed by the Committee of Sponsoring Organizations of the Treadway Commission – *Internal Control – Integrated Framework* published in 1991 has exerted considerable influence over all subsequent thinking in the field throughout the world. An institutionally strong and diffusible conception of ERM has emerged from the tradition of internal control practices. More recently another strong influence has been the Sarbanes-Oxley legislation in the United States, which has been the subject of an avalanche of criticism. While our focus here is not to review the extensive body of dialogue on Sarbanes Oxley, we note that since its inception, a significant focus around this legislation has been to enable its application and focus to be more risk-based. The Turnbull report in the UK gave further emphasis to the principles of controls, independent notification and reliance on control.

Yet such thinking has created some troublesome consequences. A model of regulatory assurance, or an 'illusion of control' (Holt, 2004), has been created by ERM designs; as long as risk has a control and a report or person dedicated to it – then somehow the risk has been mitigated. While there have been major developments in quantitative risk management tools in the financial sector, partly driven by the emergence of information technology capable of making finance theory operative, this pillar 2 emphasis on controls and 'risk governance' has had profound effects on the organizational shape of risk management (Mengle, 2003). It has become a part of regulatory common-sense.

The rise of this regulatory conception of risk management, with its origins in control thinking, can be traced in part to scandals and to policy demands for preventative solutions. COSO (1991) itself was a response to fraudulent financial reporting in the late 1980s and the

Group of Thirty drew on its ideas when it published its guidance on the governance of derivatives following the major losses in a short term account held by Orange County, (Group of Thirty, 1993). While regulatory regimes drew on these internal control systems, they also transformed them via processes of formalization and codification. In 2004, COSO updated and redesignated this control framework as Enterprise Risk Management, but the underlying logic remained unchanged.

In the next section, we elaborate further the key issues regarding these shortcomings of current ERM thinking and practice. This is followed by an example of a contrasting style of risk management visible in the work of a buy-side investment management firm. Finally, we explain why regulator driven ERM frameworks are a potential source of risk, and argue for the need to find applications more sensitive to organizational demands.

2. ERM as Command and Control

The essential structure of ERM has become a familiar part of the risk practitioner landscape. The underlying model derives control and risk management activity from the ultimate mission of the organization. This logic has a clarity and appeal which is undeniable. Thus ERM prescribes that organizations must analyze the risks to their overall objectives and determine mitigation activity based on clarity about their appetite or tolerance for the residual risks associated with their goals and sub-goals. In organizations where control activity has historically been 'out of control' as an autonomous activity, establishing a rational relationship between control investments, organizational objectives and risk appetite has an obvious attraction. At the same time, ERM articulates a strategic significance and potential for this control-based conception of risk management which it could not have done in the 1980s.

Even allowing for some variations, this idea of ERM has become part of the contemporary common sense of risk management. It is a model shared both by the large professional services firms and by regulators. It essentially reflects a model of organizational control which is similar in many respects to the principles of scientific management espoused by F.W. Taylor, which in turn influenced softer managerial forms, such as quality assurance. Just as Taylor appears outmoded today, ERM is deeply hierarchical in a way which is out of line with a great deal of recent thinking about organizations, cultures, networks and strategic

alliances. For example, although the COSO (2004) standard acknowledges the limitations of risk management and control systems, such as their vulnerability to collusion and discretionary override, its lack of organizational realism may be the most significant source of risk. This lack of realism is reinforced by regulatory demands at the operational level for the highly rationalized images of risk management which ERM frameworks provide.

It does not take much organization theory to question the assumptions underlying this misapplied notion of ERM. For example, Hood (1996) shows very clearly that models which depend on the notion of a clear risk appetite or tolerance level have an essentially 'thermostatic' or mechanical character. They assume that limits can be well-defined and can provide automatic and clear feedback to risk operatives who can make adjustments. Yet such models which work well for heating systems fail in organizations because human beings can disagree about acceptable tolerances or fail to interpret the signals properly when such limits are breached (as in the case of Three Mile Island). In a similar way, March and Shapira (1987) have shown that that decision makers do not first calculate risks and then choose among alternatives, as ERM suggests. They are also predisposed to assume that risk is manageable in a rational way, something which ERM encourages. Indeed, ERM is a mode of framing risk management which, despite qualifications, assumes that mastery is possible.

In the field of financial services, most risk management innovations arose from the sell side (at banks, investment banks and brokers) because of the sizeable principal risks they take and because of regulatory attention to conduct of business and systemic stability. Once COSO (1991) had been established as a legitimate standard, gaining accepted by the SEC, it began to acquire dominant regulatory currency, influencing the development of frameworks and templates overseas. Even apparently competing standards share much of the same structure for the organization of risk management thinking. Accordingly, the sell-side firms along with many other organizations advised by a growing consulting industry, favored and built ERM-style command and control organizations with elaborate structures of internal risk accountability.

A key aspect of the development of ERM has been the extension of value at risk (VaR) techniques to determine the risk capital needed at the aggregate level for regulatory and managerial purposes. However, VaR has its origins in the search for risk adjusted rates of return at the level of specific transactions for real clients; portfolio impacts are a macro effect of these transactions. So it is widely argued that VaR techniques are far more suitable to measure the risk

of individual positions on transactions and that there are also severe limitations of using an aggregate VaR measure. For example, there are very often attractive diversification benefits from combining portfolios that VaR does not always calculate properly. A strict reliance on only VaR will fail to provide a useful picture of extreme market conditions or the behavior of complex transactions and instruments under a wide range of circumstances which have not been historically observed.

By contrast in buy side firms, boundaries, or risk appetites, are driven from the transactions level by client guidelines – hence the management of risk is driven primarily from the 'bottom-up' by the fiduciary perspective of individual clients, rather than by some aggregate objective of the firm as whole. Relative fund performance to a benchmark is often more significant for clients than absolute performance judged by a universal risk appetite policy. In addition, portfolio managers must have discretionary execution capabilities in order to keep up with ever-changing market prices. Time of execution is measured today in microseconds. As long as the portfolio manager is within the investment guidelines mandated by the client, adding a transaction approval process actually increases risk. In short, one cannot control investment risk with a command and control paradigm like ERM on the buy side.

It is certainly reasonable to define enterprise risk as the risk that threatens the viability of the enterprise. Most of the classic cases of financial collapse and fraud have been followed by regulatory intervention to correct behavior, in particular by enhancing internal controls. In Investment Management firms the dramatology of failure is different; client risk is the main focus and the driving issue in maintaining reputation. If the client loses confidence in the enterprise's ability to manage their money effectively – for whatever the reason – the enterprise will quickly go out of business. In such a buy-side client focused world, ERM can only assume an ecological form which embodies rules "for the common good" of the enterprise. For example, client mandates may dictate that a buy-side firm should establish a maximum percent holding of an issuer. ERM should involve setting up specific "speed bumps" at certain levels to evaluate position pill provisions, regulatory filings requirements, liquidity, and relative position size versus competitors. In short, there is no gap between ERM and portfolio management; there is no need to demand the 'embeddedness' of risk management, as the UK Turnbull report does, because unembeddedness is unthinkable from the business point of view.

Similarly, in the context of a banking organization, ERM should take on a virtual environmental view in that "banks are mirrors of their environment", i.e., when there is a good economic environment their customers (consumers and corporations), do well. ERM would involve having a view of the environment and setting up "tripwires" to ensure that inflection points are noted and that the organization is not lulled into a view of the environment that has changed. For example, if a bank has a large mortgage portfolio which has on average a 60% loan-to-value underwriting criteria, when real estate values drop 5%, there should be a required time-out to review the portfolio. In essence, this kind of business-driven ERM requires the specific monitoring of external reference points that cause reflection and action. The mistaken assumption of control-based ERM is to presuppose that control indicators or Key Risk Indicators (KRIs) somehow speak for themselves. Rather the bias to action must already be embedded in triggers which demand concrete actions, initially in the form of mandated discussion. As Holt (2004: 261) suggests, risk management should be seen 'not as a way of fixing types of problem but as a mechanism for encountering problems'. The emphasis should be less on orderly models of representation and more on changes in KRIs as a provocation to the business.

In summary, control-based ERM as favored by regulators has less than optimal practicality for organizations because of its origins in frameworks like COSO which in effect assumes and produces a gap between analysis and action (Samad-Khan, 2005). Such frameworks do of course have representational functionality in so far as they provide what the regulator wants to see; they provide organizations with a way to signal conformity to abstract design principles for a risk management process, and they make this process 'auditable' (Power, 2007). But while these ERM frameworks are appealing to regulators and others, they give rise to significant practical challenges at the operational level, despite heroic attempts to align them in spreadsheets and risk maps.

3. A New Paradigm? The Case of Buy-Side Risk Management

Is it possible to generalize the case of buy-side risk management in just the same way as has happened historically on the sell side? What would our risk management discussions look like today if frameworks like COSO had never existed? In a statement of draft risk principles for asset managers (Buy Side Risk Managers Forum and Capital Market Risk Advisors, 2006), a telling footnote reports that 'aspirational programs are themselves a form of risk'. The

implication is that programs which build in a gap between analysis and actionability are a kind of operational risk. These draft principles are interesting in another sense. They are necessarily principles-based because the unique position of specific asset managers means that a rules-based approach would be instantly meaningless. In contrast most ERM frameworks lend themselves to rules-based realization. It might even be suggested that the problem of embedding risk management is exacerbated by the very frameworks designed to overcome it.

The 'counter conception' of risk management being advanced here is visible in the example of the buy-side risk management practices at AllianceBernstein (AB). AB has a chief risk officer who reports to the President and Chief Operating Officer. Each major geographical region (i.e., North America, Europe, Asia) has a senior risk manager. This relatively small unit interacts closely with other control related units, including compliance, internal audit, IT and Legal. In this AB model, the Portfolio Managers are fundamentally the first line managers of risk. They must understand the risk/reward trade-offs involved in their own investment decisions and how they become impaired when the market moves. While never perfect, the AB risk approach aims to:

- Empower senior line managers with risk management responsibility and autonomy.
- Provide clear product definitions and investment boundaries to satisfy client expectations and stated risk appetites.
- Maintain a strong, centralized new product approval process.
- Create understandable policies and procedures and ensure they are adhered to.
- Design operations so that they are driven by client needs and expectations. This entails clarifying ambiguous investment guidelines and learning from errors to ensure they do not reoccur any place in the organization.
- Promote extensive communication and dialogue about risk taking and risk management at all levels
- Sustain a governance process composed of various firm wide and business unit specific risk committees.
- Implement an industrial strength compliance function.
- Integrate the risk functions with compliance and internal audit.

The implications of this model are that the Chief Risk Officer (CRO) is not the head of an ERM bureaucracy of controls, but has 'Head of household' responsibilities which focus on specific enterprise and reputation risks. The CRO and a small, experienced team determine house limits in terms of counterparty exposure, and share ownership of these limits with managers; they provide views on who the company does business with; and they are involved in new product and financial instrument approval. In addition to this advisory and boundary setting role, the CRO exercises oversight responsibilities by subjecting portfolio management to a quarterly review to ensure that all client accounts have a statistical profile that conforms to the mandate for which the firm was engaged, and that the variation among with identical mandates falls within acceptable boundaries. In addition, the CRO is actively involved in operational risk activities since errors can undermine the confidence of clients.

Overall, the CRO team at AB operates as an internal business consultant which involves senior management in the oversight process via committee structures. The model is highly interactive; risk management is an ongoing organizational conversation which may on occasion produce tension. It includes senior management, compliance, internal audit, the Board's internal audit committee and regulators. The dynamics of the approach are critical. It does not begin with an abstract regulatory standard, but with the transactions that serve clients. Command and control is not part of daily routines in which actionability is dispersed.

The general conception of risk management underlying these activities at AB, though by no means perfect and without frictions, is very different in form from some of the other approaches used in the industry which favor centralized and prescriptively detailed conceptions of ERM. In place of creating a dashboard for an entire risk universe, a project which creates endless worries about the completeness of universe description, the focus is on surfacing problems as they arise and on resolving everyday issues by empowering the entire organization to be risk managers. The measure of success is not the ability to prove and demonstrate control universes via elaborate spreadsheets, but a singular focusing on doing the right things at the transactional level.

4. Discussion and Conclusions

It is perhaps dangerous to substitute one overgeneralization for another. However, risk management as practiced at AB and other buy-side firms has something systemic to tell us which is different in fundamental respects from the standard ERM approaches currently in fashion. ERM requires in principle the identification of all risks facing an organization, a process which may not always be possible and which ties organizations up in creating bureaucratic trails to prove the quality of process. This results in an expensive and potentially impractical description of what firms do down to the minutest detail, without prescriptions for action. The production of evidence becomes more important than managing real risks. In some cases this has also resulted in organizations adopting two kinds of risk management, one visible form for the regulator and one less visible form for the business.

It must be said that the top-down ERM approach being criticized does have a place in risk management – but only by exception when strategic or material issues may be concerned It is both a poor descriptive and normative model for the everyday need to monitor *changes* to organizational risk profile. 'Top-down' commanding approaches will certainly be relevant in emergencies, with regard to specific material transactions or to demonstrate board governance, but they lack relevance for monitoring day to day operations and are unsuitable for the decentralized structure of many contemporary organizations. A more pragmatic prescription is a 'bottom-up' approach based on defined freedoms to expand and trade subject to central tracking of relative performance that these activities remain within risk profile. The analytic and pragmatic imperative is to monitor change. Even good KRIs only tell the organization that something is changing; they must be part of defined organization prescriptions for action and review at different thresholds. In contrast, hierarchies of controls reinforce the gap between analysis and action and create alienation between the risk function and the business.

It is not surprising that most existing ERM approaches embody a rather unrealistic and outdated theory of organizations – the birds' eye view. They have little to do with organizational realities and more to do with governance design. COSO (2004) provides an idealized blueprint for an auditable risk management process, with an emphasis placed on senior management and top-down accountability. It is a prescription for a governance and accountability agenda rather than a guide to the risk management process (Power, 2004; 2007). Huge resources have been expended on establishing baseline control systems under Basel 2 pillar 2 and under section 404 requirements of the Sarbanes-Oxley legislation. Now, following

criticism, there is a move towards more 'risk-based' approaches. Yet these risk-based approaches will bring very little change in the fundamental conception of risk management. There are of course professional interests at stake: the COSO world suits accountants and consultants for whom the governance agenda of the 1990s has provided new markets. Yet despite efforts to link ERM designs to strategy, this is a world focused more on structure than business dynamics, and more on the enterprise in the abstract rather on than product creation.

In sum, practices at AllianceBernstein provide an instructive example and challenge prevailing regulatory conceptions of ERM applications. We suggest that these conceptions are the source of many difficulties organizations face in developing an intelligent risk management practice which is part of the transaction process. Though not without difficulties, the problem of embeddedness and actionability is solved under this counter conception of risk management - because there was never a gap in the first place. Control-based ERM remains attractive as a wrapper for risk governance which helps Boards discharge their duties, but it has little if nothing to say about managing risk at the point it is undertaken, and may be a source of risk to operations if it makes the risk function less credible in the business.

As for that risk person sitting before multiple computer screens turning dials and monitoring every risk in the enterprise – that individual has no place in the future of risk management. What is required is nothing less than a critical transformation in our collective thinking which we hope will mean the end of enterprise risk management as we know it today.

References

Alliance Capital. 2005. *Talking risk: the Alliance Capital Approach to Risk Management*. New York: Alliance Capital L.P.

Buy Side Risk Managers Forum and Capital Market Risk Advisors. 2006. *Risk Principles for Asset Managers*

COSO (2004). *Enterprise risk management*. Committee of Sponsoring organizations of the Treadway Committee.

Group of Thirty (1993), *Derivatives: Practices and Principles*. Washington, DC: Group of Thirty.

Hood, C. (1996), 'Where Extremes Meet: "SPRAT" versus "SHARK" in Public Risk Management', in Hood and Jones (Eds.) *Accident and Design*, London: University College Press, 208-227.

March, J. and Shapira, Z. (1987), 'Managerial Perspectives on Risk and Risk Taking,' *Management Science*' 33(11):1404 - 1418.

Power, M. 2004. *The Risk Management of Everything*. London: Demos.

Power, M. 2007. *Organized Uncertainty: Designing a World of Risk Management.* Oxford University Press.

Mengle, D. 2003a. 'Risk management as a process.' 3-10. Field, P. (ed) 2003. *Modern Risk Management: A History*. London: Risk Books

Rosen, D. 2003. 'The Development of Risk Management Software' 135-148. Field, P. (ed) 2003. *Modern Risk Management: A History*. London: Risk Books

Samad-Khan, A. (2005), 'Why COSO is Flawed?' *Operational Risk* 6(1):24-28.