The importance of systems, processes and culture

A V Vedpuriswar*

For effective Enterprise Risk Management, systems and processes must be properly designed. But equally important is culture. The organizational culture shapes the way employees perceive risks and deal with them. This article examines these issues threadbare.

A key objective of Enterprise Risk Management (ERM) is to ingrain risk management into the organisation culture by making it a core value of the organization and building it into day-to-day practices. The systems and processes of the organization should enable managers to know what risks are being taken, quantify them and assess whether they are within prescribed limits. They should also facilitate corrective action, where necessary.

The various scams and disasters in recent times (including Barings, Orange County and UBS) have made it clear that general managers cannot let treasurers and other managers operate merrily without being questioned when they are taking huge financial decisions. A system of checks and balances is necessary to keep risks within specified limits.

Along with systems and processes, it is also important to shape the culture of the organization and check dysfunctional tendencies. The 'right' culture encourages entrepreneurial risk taking but discourages gambling.

Role of the senior management

The board and the senior managers need to send strong signals that they consider risk management a priority. The board should play an active role in identifying the risks that may have a significant impact on the fulfilment of corporate objectives. It should review information on these significant risks from time to time. The board should come to a consensus regarding what risks are acceptable, the probability of their occurrence and the type of mechanisms and processes needed to reduce their impact. The board should realise that whatever be the sophistication of the control systems and processes, risks due to poor judgment, human error and unforeseen circumstances can never be completely eliminated. It should be emphasised that the role of the board is not to advocate complete elimination of risk. In a competitive market place, not taking risks could turn out to be a risk in itself. In fact, if effective risk management processes are in place, the board may decide that more risks have to be taken to exploit the opportunities available for the business to succeed in the long run.

The board and the senior management team should play an active role in the following areas:

a) **Understanding the risk profile:** The board members should clearly understand the risks to which the company is exposed. The board should further decide which risks are acceptable and which must be eliminated through the use of hedging techniques.

b) **Setting policy:** The board should prepare policy guidelines, including the corrective action to be taken when things go wrong. For example there should be guidelines on when and how to unwind

* *A V Vedpuriswar, Consulting Editor, Global CEO is also Dean, ICFAI Knowledge Center.*

an unprofitable position, if rates move unfavourably. The exit strategy should be based on the amount of money the company is willing to put to risk.

c) **Establishing controls:** Steps should be taken to ensure effective implementation of policies. An independent risk management unit is desirable. Ideally, risk managers should not report to traders. It is a good practice to make risk managers report to people one level higher than those who execute and approve derivative transactions.

d) **Setting up systems:** The most expensive but integral part of a comprehensive risk management function is consolidation and integration of data from a number of different systems across the company's operations.

e) **Checking compliance:** The risk manager should send reports regularly to the senior management and the board. These reports should check compliance with policies and procedures and make independent evaluations of the various derivatives positions. The reports should also indicate whether the positions are synchronous with the company's accounting department and with the disclosures in the company's financial reports.

f) **Periodic review:** The board must make it clear to traders and treasury managers that any violation of policies, guidelines or controls will be punished. When limits are violated, the board should not hesitate to take immediate action and send clear signals that indiscipline will not be tolerated.

Aligning control systems with corporate strategy

Many of the risks which organisations assume are man made. Fluctuations in the environment do create uncertainty. But, how to deal with this uncertainty is in the hands of the organisation. Some companies take disproportionate risks in their endeavour to maximise returns. Enron, which has recently gone bankrupt is a good example. Others take less risks and are happy with moderate returns. So, it is necessary to quantify as many parameters as possible and lay down guidelines for employees on the amount and type of risk they can assume and how they must manage these risks. An effective management control system provides the necessary checks and balances.

A well designed organisational structure, effective reporting systems backed by the requisite IT infrastructure and well thought out compensation and incentive plans are integral components of a good control system. A well-designed management control system ensures that there is internal consistency between the company's long term objectives and day to day operations.

It is a good practice to make risk managers report to people one level higher than those who execute and approve derivative transactions

The starting point in designing the management control system is a good understanding of the company's strategies. The following questions should be asked:

1. Is the strategy internally consistent?
2. Is the strategy consistent with the environment?
3. Is the strategy appropriate in view of the available resources?
4. Does the strategy involve an acceptable degree of risk?
5. Does the strategy have an appropriate time horizon?
6. Is the strategy workable?

A strategy should be consistent both with the environment and with the organisational goals and objectives. Strategy formulation should keep in view the resources available and the risk-taking capabilities of the management. Appropriate criteria should be developed to assess whether the strategy will work given the organisational capabilities. Since implementation of strategy involves commitment of resources, the management should determine the time frame over which a given strategic choice will have its impact. This is necessary to understand whether the company has adequate staying power till the strategy is satisfactorily implemented.

Planning and control play a important role while implementing any strategy. The management first decides what the organisation plans to achieve in a given time period. This is the planning aspect. Next comes the measurement of what is happening. Managers have to decide whether the difference between the desired state and actual state is significant or not. Accordingly, they need to take corrective action, where necessary. This is the control aspect.

Control systems in an organization typically involve the following functions:

i) Planning

ii) Coordination

iii) Information sharing and reporting

iv) Deciding the action to be taken based on targets and performance

v) Influencing people, changing their behaviour and aligning their goals with those of the organisation.

Control systems should align individual and corporate objectives and discourage excessive risk taking

Control systems should align individual and corporate objectives and discourage excessive risk taking. For example, the annual bonus of a treasurer should not be based solely on the profits he or she generates. It should take into account the riskiness of the activities undertaken and the contribution the treasurer has made to non trading activities. The collapse of Barings was due to a divergence between individual and corporate objectives.

While on the subject of strategy formulation and implementation, let us note that an organisation has three broad layers, corporate management, divisional management and operating management. The corporate management is responsible for the performance of the organisation as a whole. The divisional management is responsible for the performance of geographic regions or product divisions. The operating management takes care of day to day activities and is responsible for the accomplishment of specific operational tasks. The type of risks each layer has to manage is different though there may be overlaps.

The importance of management information systems

A management control system will be ineffective without relevant information. To monitor and control risk, information should be easily accessible. Management Information Systems (MIS) help in collecting, processing and presenting information to the management to help take better decisions. A good MIS forms the backbone of any risk management system.

The presentation of the information will depend on the managerial level at which it will be used and how the information is generated. Strategic planning relies heavily on external information. Management control largely uses data generated within the organisation. Operational control uses data generated in the context of specific tasks or activities. Data generated during the process of strategic planning may not be very accurate, because of the uncertainties involved. Data generated in the case of management control and operational control is more accurate and reliable because they relate to events taking place currently or which have taken place in the immediate past.

A good MIS provides both financial and non financial information in a user-friendly form, highlighting the critical factors. In general, MIS generates two types of reports – control and information. Control reports focus on the comparison of actual performance with standard performance. Information reports give information about the state of affairs at periodic intervals. An effective MIS should be timely, accurate and relevant. It should provide the right information, in the right place, at the right time and at a reasonable cost.

The role of Auditing

Continuous monitoring is necessary to ensure the integrity of risk management controls and systems. Auditing and testing should be undertaken periodically to check the robustness of the systems, procedures and controls. Audits are used to set standards and assess the effectiveness and efficiency of the system in meeting these standards. They help managers to

identify the scope for improvement and act as a reality check by assessing how organizational processes are working. Sometimes, audits may identify outdated strategies.

A comprehensive audit reviews all the processes associated with measuring, reporting and managing risk. It verifies the independence and effectiveness of the risk management function and checks the adequacy of the documentation. Audits should be held regularly to take into account changes in the circumstances and to monitor progress. The frequency of audits would depend on how integral it is to the company's strategy, the time and expenditure involved, etc. Audits can be performed in various ways – surveys, questionnaires, focus groups. Audits however cannot mobilize people into action. Indeed, in some of the classic failures like Barings and Bhopal, audit recommendations were not implemented.

Integrating risk management with structure, culture and processes

The focus on risk management needs to be reflected in the organization's structure, culture and processes. The organisational lines of responsibility and authority need to be established and communicated clearly. A single point source of responsibility that acts as a check on risky strategies is desirable. Thus, a Chief Risk Officer's (CRO) post should be created. The CRO should be empowered to impose checks and balances wherever appropriate. A clear set of corporate objectives and strategies that indicate the acceptable attitudes to risk taking and the establishment of guidelines within which the various trading and operating units should function is also a must.

Organisational processes and procedures must be designed according to corporate priorities and goals rather than regulatory requirements. While they must provide the necessary checks and balances, they must also empower the staff and facilitate quick but informed decision making instead of entangling them in red tape and bureaucracy.

A company's culture is nothing but the shared beliefs, values and perceptions held by its employees. In a strong culture, these values and beliefs are shared widely by employees and evoke strong commitment. Culture facilitates control by developing a sense of group loyalty and by reducing dissonance. Indeed, self control through the acceptance of common values can be a very effective control system. However, strong cultures can also create problems while managing change. In general, strategy and culture must be consistent.

For businesses to prosper, entrepreneurial risk taking is necessary. Yet, too much risk taking can lead to a gambling mentality. The 'right' culture ensures that employees do not put the future of the company at stake in their drive to achieve results. So, when organizations design reward systems for achievers, they also need to have checks and balances to monitor the way in which results are being achieved.

For businesses to prosper, entrepreneurial risk taking is necessary. Yet, too much risk taking can lead to a gambling mentality

In cultures, where the 'boss knows best' and the top management doesn't take bad news or constructive criticism in the right spirit, things can go seriously wrong all of a sudden. If there is a tendency to keep looking at employees who report bad news, as trouble makers and poor team players, problems will remain hidden under the carpet. Over a period of time, such an attitude will have a significant negative impact. Reputed Fortune 500 companies like General Motors, Kmart and IBM have all run into problems at some point of time or the other because of the shoot-the-messenger syndrome.

When employees perceive their career progression as a zero-sum game and think it is I or he, unintended consequences often result. Poor information sharing and lack of coordination are quite common in such situations. Not only that, in their determination to get ahead of their peers, employees may try to improve their short term performance by indulging in acts which may harm the company in the long run.

In some cases, wrong signals sent by the top management result in dysfunctional decision making. In the Union Carbide factory in Bhopal, for example,

local managers in their efforts to cut costs in a loss making operation, decided to violate even the most elementary safety measures.

Gary Hamel[2], emphasises the need to encourage 'activists' in an organisation. Activists are prepared to challenge conventional wisdom and come up with new revolutionary ideas that form the basis for radical innovation. They do not hesitate to tell the truth. They are fiercely committed to the whole organisation. They want the organization to benefit from the new idea. They are courageous and are not afraid to speak for what they stand, even at the risk of offending the top management. A good example is Sony's Ken Kutaragi, the architect of Playstation II. Hamel refers to Kutaragi as a digital bandit. Activists are pragmatic and want to make things happen by starting on a small scale rather than waiting for grandiose projects to be approved. Today, the challenge for most organisations is to shape the culture in such a way that a sufficiently large number of activists are around to keep looking at new things or to look at existing things in a different way.

Knowledge sharing and Risk Management

Much of the literature on risk management has focussed on strengthening the control systems and modifying incentive programs. The assumption is that checks and balances combined with the 'right' incentives will limit risk to manageable proportions. Yet, it is very often the way the knowledge of an organisation is shared between traders and the senior management that determines a firm's capacity to deal with risk.

By its very definition, risk means vulnerability. Especially in the case of financial risk, much of the vulnerability is due to external fluctuations in commodity prices, interest rates, foreign exchange rates and so on. A threshold level of knowledge is critical in anticipating and interpreting these events. Many of the biggest financial disasters in recent times have been partly, if not completely, due to ineffective knowledge management practices.

To tap knowledge effectively and leverage it for the benefit of the organisation, capabilities have to be

Identifying and Assessing Risk from an ERM Perspective

The CEO and the board of directors should consider a number of questions during risk identification and assessment. Such questions include:

Strategic Risk	Are the critical strategies appropriate to enable the organization to meet its business objectives?
	What are the risks inherent in those strategies, and how might the organization identify, quantify, and manage these risks? How much risk is the organization willing to take? What risks result from e-business developments?
Operational Risk	What are the risks inherent in the processes that have been chosen to implement the strategies?
	How does the organization identify, quantify, and manage these risks given its appetite for risk? How does it adapt its activities as strategies and processes change?
Reputation Risk	What are the risks to brand and reputation inherent in how the organization executes its strategies?
Regulatory or Contractual risk	What risks are related to compliance with regulations or contractual arrangements—not justthose that are financially based?
Financial Risk	Have operating processes put financial resources at undue risk? Has the organization incurred unreasonable liabilities to support operating processes? Has the organization succeeded in meeting measurable business objectives?
Information Risk	Is our data/information/knowledge reliable, relevant, and timely?
	Are our information systems reliable?
	Do our security systems reflect our e-business strategy?
New Risks	What risks have yet to develop? (These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk disasters (rogue traders), and other crisis and disaster risk).

Source: kpmg.com

2. Leading the Revolution.

built in generating, accessing, transferring, representing and embedding (in processes, systems and controls) knowledge. In sum, what is needed is an organisational culture that values, shares and uses knowledge.

Rapid rates of technological obsolescence, globalisation, deregulation and increasing volatility in the financial markets have increased the vulnerability of companies and put a premium on knowledge. It is not that knowledge does not exist within the organization. It exists, but within the brains of a few people such as traders and treasurers. The challenge is to capture this knowledge and make it available to other employees to facilitate the process of organizational learning. As Marshall, Prusak and Shpilberg[3] put it, "Fundamentally, risk management is about managing the complexity inherent in the trade off between return and risk, through organisational knowledge, for the benefit of the firm's stakeholders."

While a scientific, rational approach to risk management is desirable, it is equally important to understand the behavioral issues involved

Consider a large MNC. For its financial risk management practices to be effective, the senior management and the treasury would need to have shared beliefs about expectations of the future, risk disposition, riskiness of the hedging strategy employed and the acceptable pay back period. In the case of Metallgesellschaft, the German oil refining and trading company, the headquarters and the US subsidiary were not aware of the different accounting standards in the two countries. Looking back, a mechanism to share knowledge between headquarters and the subsidiary, might well have averted the crisis.

Traders gain insights as they operate in the markets and interact with other market participants. Such knowledge influences their individual decision making processes. The challenge for organizations is to capture this knowledge and share it with other managers in the system, so that they have a reasonably good understanding of what is going on at the trading desk. As Marshal, Prusak and Shpilberg[3] put it, "An excess of control systems can also produce an illusion of control, hiding the very real risks that lie in those areas where much that is not quantifiable or constant must be factored into a decision, in which onus is on good contextual knowledge to reduce the inevitable ambiguity. A plethora of controls will not help a trading operation if traders do not share contextual knowledge about their insights with their managers or if traders operate with assumptions that differ from the equity holders of the firm."

Many of the quantitative models which treasurers and derivative traders use, incorporate various forms of knowledge. What must be kept in mind here is that knowledge is not static. It should be frequently upgraded by questioning the assumptions behind the model as conditions in the environment change. It is the frontline employees, the traders who first come to know what is happening outside. So systematic efforts must be made to collect their insights and disseminate it so that the senior management has a grip on what is happening. The senior management should also spend some of its time in face to face interaction with the traders. This helps in transfer of implicit knowledge which is difficult to document and transmit in the form of reports.

Concluding Notes

In this article, we focussed on some of the 'soft' issues in risk management. We tried to understand the role played by systems, processes and culture in encouraging/discouraging employees in an organization to take risks. While a scientific, rational approach to risk management is desirable, it is equally important to understand the behavioral issues involved. Ultimately, it is the actions of individual managers, which make or break a company. A deep understanding of the decision making processes is necessary to put in place the required systems and processes. Indeed, systems and processes by monitoring risk systematically can actually facilitate more risk taking. A supportive organizational culture can motivate employees to take calculated risks but without throwing caution to the winds. Shaping a culture is a long-drawn-out process but time and effort must be invested to align culture with the company's long-term strategy. A dysfunctional culture can bring a company to ruin.n

Reference 15-02-10-05

3 California Management Review, Spring 1996, pp. 78-101.