An Introduction to Enterprise-Wide Risk Management

Anup Kumar Agarwal

The author is AGM, ICRA Management Consulting Services. He can be reached at anupagarwal@hotmail.com

Perhaps the one question that regularly haunts every single CEO, whether of a manufacturing company or a service organisation, is: "Would we be able to achieve our business and financial objectives?" The question, however phrased, is often a part of a chain, with the succeeding ones being: "What is it that could stand in the way of the objectives being achieved? Actually, what are the risk-factors facing our company? How significantly can the risk-factors hinder the achievement of our objectives? Can these risk-factors be mitigated? Can we regularly control and monitor the risk-factors?…"

The solution to such troublesome queries probably lies in Enterprise-Wide Risk Management (EWRM). EWRM is a continuous and structured process of identifying all external and internal risk-factors; assessing the impact of each of these risk-factors on the achievement of an organisation's objectives; prioritising the risk-factors; exploring options for mitigating the risks; and controlling and monitoring such risks.

EWRM is not limited to one event or circumstance. It is a dynamic process that unfolds over time and permeates every aspect of an organisation's resources and operations. It involves people at every level and requires applying a portfolio view of risk across an entire enterprise. By embedding risk management techniques in its day-to-day operations, an enterprise is better equipped to identify events affecting its goals and manage risks in ways that are consistent with its risk appetite.

> The EWRM is a continuous and structured process of exploring, identifying and analysing all external and internal risk-factors and finally to mitigate its probability in a focused, coordinated and well-planned manner. It usually demands a cultural change in an organisation at every level.

Simply put, an organisation could follow these steps while implementing EWRM:

1. Look at each of the objectives;
2. Identify the risk-factors that could affect the achievement of each of the objectives;
3. Assess the impact of the risk-factors on the achievement of each of the objectives;
4. Explore options for mitigating the risk-factors;
5. Identify champion(s) in the organisation to regularly control and monitor the risk-factors.

Let us take an example. Assume today is October 1, 2004, and one Mr. A staying in Mumbai wants to reach Delhi on October 5, 2004 by 10 a.m. If he takes the 8 a.m flight from Mumbai on October 5, he would reach Delhi by 10 a.m.

Now, Mr. A clearly has two options:

1. To take the 8 a.m flight and not bother about reaching on time
2. To assess the risks of taking the 8 a.m flight.

If he chooses the second option, he identifies the following major risk-factors that can affect the achievement of his objective, which is to reach Delhi on October 5, 2004 by 10 a.m:

- The flight does not take off on time
- The flight takes off on time but does not land on time because of delayed landing clearance, or fog or some such reason.

Now, the reason that Mr. A has to reach Delhi by 10 a.m is that he has to attend a business meeting that starts at 10.30 a.m. In case he is late, the business opportunity may well be lost and the loss could be significant. If such is the case, the impact of the risk-factor is clearly quite high.

The question now is: Can these risk-factors be mitigated? The answer is of course "yes". The risk mitigating options could be:

- Mr. A takes the 7 a.m flight or an even earlier flight on October 5, 2004

- Mr. A. travels the previous night.

Mr. A may also monitor the actual flight departure and arrival timings for the 8 a.m flight till October 4, 2004 and then choose the flight he would take. He may also like to carry out a cost-benefit analysis for each of the options.

We have all faced Mr. A's situation. And many of us may have also suffered the consequences of choosing or not choosing a particular option.

Let us now take the example of an organisation. Essentially, the process is no different for it.

Assume,

- Company XYZ's objective is to hit a sales target of Rs. 100 crore in 2004-05.
- One of the risk-factors identified by XYZ that could affect its objective is "untrained marketing team".

XYZ knows that if it does not have a well-trained team in place, it would at most achieve sales of Rs. 70 crore, which is marginally higher than previous year's sale. This shows that "untrained marketing team" is a major risk-factor. There could be other risk-factors too, like competition, regulation, and lack of brand pull.

Now let us explore a few risk-mitigating options for "untrained marketing team". The options could be:

- Train the existing marketing team
- Hire well-trained personnel from the market
- Use a mix of the two

For each of the above options, XYZ should carry out a cost-benefit analysis before choosing a particular option.

The question now is: Do all organisations follow this process of risk management? The answer is, while the process is followed by many organisations in silos, it is not followed enterprise-wide on a regular basis. The difference between a silo-based approach and EWRM is that in a silo-based approach few risk-factors are identified and addressed, while in EWRM all risk-factors are identified and addressed. Implementing an enterprise-wide process is a challenge and requires understanding, willingness, and the commitment of the top management.

I sometimes wonder why some companies do better than others? The answer probably lies in the way the better ones manage risks. The better companies are probably able to identify risks, assess the impact of the same on their objectives, and mitigate the risks. Also, it is often noticed that some companies do well for a few years and then perish.

EWRM is not limited to one event or circumstance. It is a dynamic process that unfolds over time and permeates every aspect of an organisation's resources and operations. It involves people at every level and requires applying a portfolio view of risk across an entire enterprise

Lamiya Lokhandwala

The reason probably is that they were not able to identify the risk-factors at the right time, and thus succumbed to them eventually. But it is also true that some companies have survived for decades and even centuries. Probably these have been able to identify the risk-factors and take adequate risk mitigating measures.

The better companies are probably able to identify risks, assess the impact of the same on their objectives, and mitigate the risks. Also, it is often noticed that some companies do well for a few years and then perish. The reason probably is that they were not able to identify the risk-factors at the right time, and thus succumbed to them eventually

Risk was always an integral part of business in the past, and so it is today. But the levels of risk have increased nowadays because of the increasing pace of change in the operating environment. In today's uncertain and volatile business world, managing risk more coherently, comprehensively and economically through effective enterprise risk management is simply critical.

EWRM enhances an organisation's capability to enhance risk response decisions, minimise operational surprises and losses, rationalise capital, and deal effectively with potential future events that create uncertainty.

EWRM can be applied to all entities, regardless of size. The methodology for implementing EWRM is likely to be less formal and less structured in the case of smaller entities than larger ones, but the basic concepts would be the same.

EWRM may be considered in the context of an enterprise as a whole, or for one or more of its individual units. A company may have joint ventures, partnerships or other investments, the operations of which may not be under the company's direct control. In considering the effectiveness of the company's EWRM, one would also need to look at the extent to which the company and the investment vehicle together have adequately applied EWRM, in the light of the company's strategy and related objectives.

As a first step towards implementing EWRM, organisations should do the following:

1. Evaluate the existing risk management systems
   (a) Review the internal environment with a view to assessing the risk philosophy and risk culture
   (b) Review the process of setting objectives
   (c) Assess the existing mechanism of identifying risk-factors that can affect achievement of the desired objectives
   (d) Evaluate the existing process of assessing risks
   (e) Assess the process of responding to identified risks
   (f) Evaluate the adequacy of existing control processes
   (g) Assess adequacy of existing management information system (MIS)
   (h) Review the process of monitoring risks
2. Formulate a road map for the implementation plan that seeks to bridge the gaps in risk management practices vis-à-vis EWRM.

The above steps are elaborated below.

1a) Review the internal environment with a view to assessing the risk philosophy and risk culture

An enterprise's internal environment is the basic foundation of its risk management framework. As a starting point, an organisation therefore needs to review the following to understand the prevalent internal environment in the organisation:

- Risk philosophy and risk appetite
- Risk culture and risk sub-cultures
- Recognition of risk reality
- Independence and involvement of board of directors
- Commitment to competence
- Management's philosophy and operating style
- Organisational structure
- Assignment of authority and responsibility
- Human resource policies and practices

1b) Review the process of setting objectives

Risk management should be with respect to the set objectives. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks. Objective setting is a precondition to risk identification, risk assessment, and risk response.

An organisation needs to get answers to the following questions:

- Is there a process of setting objectives?
- Are objectives aligned with strategic goals?
- Are the strategic goals consistent with risk appetite?
- In considering alternative strategies to achieve its strategic objectives, does management identify risks associated with a range of strategy choices and consider their implications?
- Is there a process of setting risk tolerance limits?

1c) Assess the existing mechanism of identifying risk-factors that can affect achievement of the desired objectives

A multiple of external and internal risk-factors could potentially affect strategy imple-

mentation and achievement of objectives. As part of EWRM, personnel should recognise the importance of understanding external and internal factors and the type of risks that can emanate there from. Management should consider current factors, as well as those that may occur in the future.

Few examples of external factors include:

- Economic and Business – Related events might include emerging competition and market movements.
- Natural environment – Events might include such natural disasters as flood, fire or earthquake.
- Political – Events might include newly elected government officials, political agendas and new legislation and regulations.
- Social – Events might include changing demographics, new food harvesting and preparation methods, and shifting family structures and work/life priorities.
- Technological – Events might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

Risk-factors also emanate from choices management makes about how it will function. The entity's capability and capacity reflect previous choices, influence future events and affect management decisions.

Few examples of internal factors include:

- Infrastructure – Events might include unexpected repair costs, or equipment incapable of supporting production demand.
- Personnel – Events might include high attrition rates, frauds, increased human error.
- Process – Events might include product quality deficiencies, unexpected downtime, or service delays.
- Technology – Events might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.

The focus should be:

- Whether there is a process of identifying external and internal factors that influence events?
- Is there a process to assess their significance?
- Has any link been established between the internal and external factors to the identification of potential events that impact objectives.
- What types of techniques are used to identify events like building databases or conducting interactive group workshops?
- What is the periodicity of identifying such events – ongoing or periodical?

1d) Evaluate the existing process of assessing risks This process focuses on both the likelihood and impact of potential events and their effects on objectives. While a single event's impact might be minimal, a sequence of events can magnify its significance.

Risk assessment employs both qualitative and quantitative methods—and evaluates potential uncertainties as they unfold, whether they are internally or externally generated.

The focus should be on the following:

- Whether a process of assessing likelihood and impact of potential events exists?
- Which methods are used for risk assessment – qualitative or quantitative?
- Whether organisation follows stress testing and scenario analysis?

1e) Assess the process of responding to identified risks Once risks have been identified and categorised, management should evaluate possible responses and their effects. Options should be weighed in relation to both risk

Risk was always an integral part of business in the past, and so it is today. But the levels of risk have increased nowadays because of the increasing pace of change in the operating environment

appetite and cost vs. benefit models. For effective risk management, managers must select a risk response that is within the parameters of risk tolerance.

Risk responses typically fall into four categories: avoidance, sharing, reduction and acceptance. Management should consider actions based on the response categories cited above. Once management selects a risk response, it shifts into action, developing an implementation plan to respond and then reassess residual risk.

1f) Evaluate the adequacy of existing control processes Control activities mean the policies and procedures that help in ensuring that risk responses are carried out. Control activities should occur throughout the organisation, at all levels and in all functions. They include a range of activities – as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

The focus should be on the following:

- What are the types of control activities followed by the organisation?
- Preventive/detective/manual/automatic
- What types of policies and procedures are in place?

1g) Assess adequacy of existing management information system (MIS)

Information is needed at all levels of an organisation to identify, assess and respond to risk. Pertinent information from both internal and external sources must be captured and shared in a form and timeframe that equips personnel to react quickly and efficiently. Effective communication would also involve the exchange of relevant data with external parties, such as customers, vendors, regulators and shareholders.

EWRM can be applied to all entities, regardless of size. The methodology for implementing EWRM is likely to be less formal and less structured in the case of smaller entities than larger ones, but the basic concepts would be the same

Effective EWRM relies on both historical and current data. Historical data tracks actual performance against targets, identifies trends, correlates results and forecasts performance. Historical data also provides early warning signals concerning potential risk-related events. Current data gives management a real-time view of risks inherent in a process, function or unit. This enables an organisation to alter its activities as needed in keeping with its risk appetite.

The focus should be on the following:

- What are the types of management information systems?
- What is the depth and timeliness of information captured?
- What is the quality of information – current/correct/accessible?
- What mechanisms are followed for internal and external communications?

1h) Review the process of monitoring risks Monitoring ensures that the components of EWRM are applied at all levels. Monitoring generally occurs in two ways: on an ongoing basis or via one-time evaluations. Ongoing monitoring is performed in real time, responds to changing conditions and is embedded in operations. Since one-time evaluations take place after the fact, problems are targeted more quickly by ongoing monitoring systems.

The focus should be on the following:

- Whether monitoring is ongoing or one-time?
- What is reported and to whom it is reported?
- What is the scope and frequency of monitoring?
- What types of evaluation methodologies and tools are used like checklists, questionnaires and flowcharting techniques?

2) Formulate a road map for the implementation plan that seeks to bridge the gaps in risk management practices vis-à-vis EWRM.

After an organisation conducts a thorough gap study of its existing risk management practices, it needs to draw up a roadmap to move towards EWRM. The road map should include timelines, milestones and responsibility centres for achieving the desired form of EWRM.

Will EWRM provide a complete solution? While the concept looks appealing, its implementation will be the key to success. ❐