Chapter 2: LITERATURE REVIEW

Chapter Highlights

This chapter presents the review of literature and will endeavor to unravel the various definitions of ERM, study the popular works on ERM framework including the COSO ERM framework, ERM works and surveys in the various industries in tandem with other relevant processes and concepts needed to appreciate the framework and the growing influence of Enterprise Risk Management as a hot topic from class room to Board room. The paradigm shift in traditional risk management from silo based to portfolio based approach and the espoused design philosophy of the ERM system for an organization replete with risks are presented to get a deeper appreciation of ERM from internal and external perspectives along the risk continuum. The review will concentrate on the implementation initiatives thus far in the oil & gas industry and in particular explore the focus on Middle East Oil Industry. Based on a critical synthesis of previous research, published articles and commentaries the various gaps in the Literature are finally established to set out the Research Questions.

Contents

2.0 Works on Enterprise Risk Management

A literature review is an account of what has been published on a topic by accredited scholars and researchers, conveying what knowledge and ideas have been established on a topic. It provides the relevance to a particular issue, area of research, or theory, providing a description, summary, and critical evaluation of each work. The purpose of this section is to offer an ***overview of significant literature published on a topic*** (Cooper, 1998; Galvan 1999). While Bourner, (1996) adds that there are good reasons for spending time and effort on a review of the literature before embarking on a research project.

The objective of this literature review (Bourner, 1996) is to give an overview of the recent studies devoted to the topic of Enterprise Risk Management. Although my attention goes primarily to publications that investigate the various links for better implementation of the ERM system, I have taken into account a wider spectrum of issues related to understanding ERM itself as it is a ***contemporary hot topic*** (Deloitte, 2008). The other reason for this approach is that the concept of ERM also permeates in all directions of any organization.

Hart (2000) recommends that a literature review is the ***effective evaluation of selected documents*** on a research topic. A review may form an essential part of the research process or may constitute a research project in itself. In the context of a research paper or thesis the literature review is a ***critical synthesis of previous research***. The evaluation of the literature leads logically to the ***research question***. Furthermore, I am interested to acquire an overview of ERM implementation in a wholesome way as this will allow me to examine the literature for the unanswered questions and gaps for further research.

ERM being a contemporary topic is a new concept in the industry and the top management buy-in for this topic has just warmed up in various sectors apart from the actuarial and banking sectors. It is indeed currently regarded as a hot topic in academia especially in management science and applied management disciplines. The background research for such a topic becomes a challenge in itself as there is no copious data available through scholarly articles with the emphasis being on ERM and its focus on oil

& gas industry. Notwithstanding this disadvantage, earnest efforts have been made to collate and investigate all the relevant information possible, which can be of significance in my academic work. It also provides an opportunity to add credible knowledge to the Body of Knowledge on enterprise risk management.

Despite the importance given to traditional risk management in a silo based approach, most of the professional and scholarly literature on ERM has only recently focused on the portfolio approach to risk management. Many studies are focused on anything from different applications and methodologies entrenched with risk jargons to aspects of mathematical analysis of risk. Studies that view risk in a holistic fashion so that strategic business decisions can be made with confidence is few and far between and the risk fraternity is catching up in closing this academic gap. It has been widely acknowledged in many publications that 'Risk' to people with different backgrounds in different organizations and industries are completely different. Risk to a risk manager in a bank versus an actuary in an insurance company versus a risk person working in a large mining conglomerate, although it's the same word, it is completely a different topic. They all look with different perspectives and that is the ***major reason that we do not have a consistent definition of what ERM is and how we implement it*** (Deloitte, 2008). Perhaps even the Big Fours would not be able to make a package and sell the perfect ERM solution because there is still none yet, although the need to follow the system is driven by regulators. It finally boils down to a broad brush adage 'it just makes good business sense!' to implement an ERM system. Psica (2008) states that, 'as ***an emerging business practice***, it is unrealistic to expect organizations to have fully developed their ERM capability.'

As indicated in the Introduction, a seminal idea in the creation of a new theory on risk management has been promulgated by COSO in 2002. The articles and reports being published by COSO members and other professional 'Risk' bodies have been accessed to cull out relevant literature review material to identify and later on emphasize on the most inter-related factors focusing on better implementation of ERM system. Accordingly, Tueten (2005) states that, 'In terms of the practical implementation of ERM in a

company, a lack of precedent, standards, and methodology in legislation leaves the situation wide open with little guidance. One document, Enterprise Risk Management – Integrated Framework, published by the COSO, provides some initial structure for such an implementation ***but lacks practical advice*** for the application of its principles.' Clearly, this suggests that there is scope here for a great deal of more research to understand the implementation requirements of ERM. Furthermore, a combination of ERM and Oil industry or Energy industry has attracted considerable attention in recent years especially with various Management Consultants. Surely a study of ERM application on the oil titans of the Middle East is a new area to be worked upon. However, in contrast to what has been inferred in various articles, it has also been observed that, in the last few years, prompted largely by the work of COSO ERM framework (2002), numerous articles have appeared highlighting the benefits of ERM, achieving Turnbull and drivers to ERM, interrelations with Basel II, Solvency II and SOX 404 compliance issues, and also how ratings companies contend with the assessment of ERM implementation etc, the cost of implementation is phenomenal and only bigger organizations can embrace such a system.

2.1 Definition of ERM

According to a Deloitte Report (2008), 'From the boardroom to the classroom to the newsroom, Enterprise Risk Management is a hot topic, yet despite this widespread awareness, a standard definition of ERM remains elusive, and the range of practices falling loosely under the heading of ERM is vast and growing'.

Based on narratives gleaned from a Marcus Evans Conference, London, (2007), some of the positive set of definitions is presented below.

- "A strategic discipline which enables a firm to take a holistic view of all risks facing the organisation.....to 'reduce surprises'..."
- "Identification of major risks to the company and follow-up of the implementation of the action plans to counter those risks."

- "Complex view on all risk relevant issues that concern the company's doings and activities."
- "Total integrated way of managing risks that translates in effective and informed decision making process."
- "A safety system for stakeholders."

- ***"Inclusion of risks from all sources and exploitation of the natural hedges and portfolio effects from treating risks in the collective."***

-(Institute of Internal Auditors Research Foundation,2001)

- "Understanding the key risks facing the entire organisation, and aggregating this information, so that the right decisions can be made about where to allocate capital to facilitate business improvement."

- ***"... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."***

- (COSO ERM – Integrated Framework, 2004)

And a cynical one

- "Jargon used by Management Consultants who are usually trying to sell you something you don't need."

2.2 The COSO Cube

Underlying Principles of ERM

The underlying principles of ERM as explained by IIA is that, 'every entity, whether for-profit or not, exists to realize value for its stakeholders. Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day. ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

The above principles consequently justify the need for an ERM in any entity.

Today's organizations are concerned about:

(1) Risk Management

(2) Governance

(3) Control

(4) Assurance (and Consulting)

According to the IIA, the COSO model provides an excellent framework that can be leveraged to think about broader risks facing the enterprise, beyond just reporting risks in isolation. The COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management, which leads to the three dimensional matrix, in the shape of a cube, also referred as the ***COSO Cube*** (See Fig. 2.1).

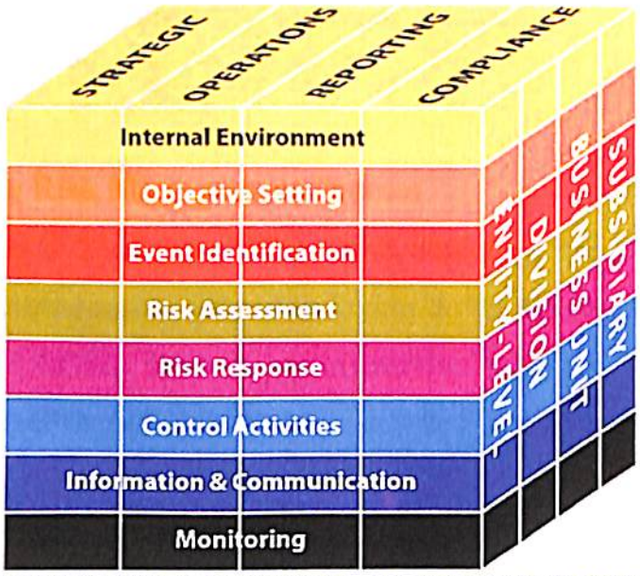

Fig. 2.1 'COSO Cube', Adapted from ERM Framework by Committee of Sponsoring Organisations of the Treadway Commission (2004)

The cube is an interaction of the components of ERM, across the organization's (entity's) objectives and the entity's units as depicted in the third dimension of the cube.

The Risk Universe

Axis – 1 of the COSO Cube depicting the ERM framework is geared to achieving an entity's objectives that can be viewed in the context of four ***categories***:

- **Strategic** : *high level goals, aligned with and supporting overall mission.*
- **Operations** : *effective and efficient use of resources.*
- **Reporting** : *reliability of reporting.*
- **Compliance** : *compliance with applicable laws and regulations.*

The above four categories are also referred as ***Risk Universe*** in the industry by Management Consultants, in the context where the risks are inventoried from the above categories. The risk universe will ultimately become a dynamic portfolio of risks. By the very nature of this inventory and the degree of risk information accumulated, the universe is a powerful knowledgebase providing the structure for comprehensive monitoring and reporting of an entity's universe of risks.

The Risk Management Process

Axis – 2 of the COSO Cube depicting the ERM framework, comprising of the ***Risk Components*** is geared to laying down the steps to the generic risk management process. The COSO cube is an interaction with the various components of ERM across the Categories of the entity as discussed below.

1. **Internal Environment** - The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

2. **Objective Setting** - Objectives must exist before management can identify potential events affecting their achievement. ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

3. **Event Identification** - Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective setting processes.

4. **Risk Assessment** - Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed; Risks are assessed on an inherent and residual basis.

5. **Risk Response** - Management selects risk responses- avoiding, accepting, reducing, or sharing risk - developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

6. **Control Activities** - Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

7. **Information and Communication** - Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities; Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

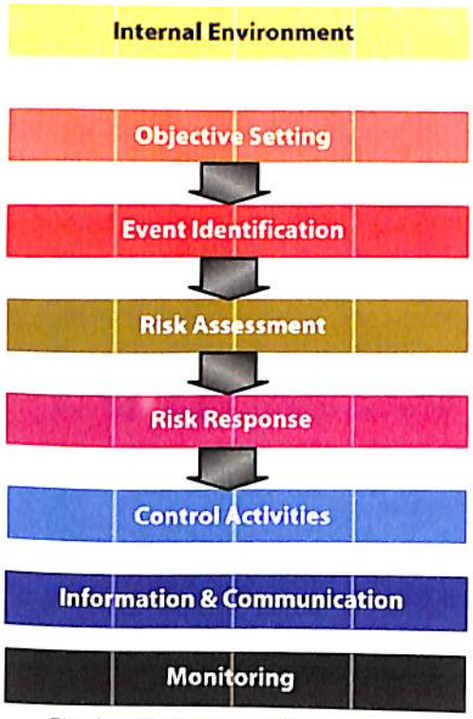

Fig. 2.2, 'Expansion of Components'
Adapted from COSO ERM Framework (2004)

8. **Monitoring** - The entirety of enterprise risk management is monitored and modifications made as necessary; Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

The COSO ERM framework states that Objective Setting, Event Identification, Risk Assessment and Risk Response represent a process flow (See Fig. 2.2) in the COSO Cube. Internal Environment, Information & Communication and Monitoring components are stand alone features of an entity.

Furthermore, COSO also states that ERM is a dynamic process. The assessment of risks drives risk response and may influence control activities and highlight a need to reconsider information and communication needs or the entity's monitoring activities. Thus, ERM is not a serial process, where one component affects only the next. It is a multidirectional iterative process in which almost any component can and will influence another. No two entities will, or should, apply ERM in the same way. Companies and their enterprise risk management capabilities and needs differ dramatically by industry and size, and by culture and management philosophy. Thus, while all entities need each of the components to maintain control over their activities, one company's application of the ERM framework – including the tools and techniques employed and the assignment of roles and responsibilities for ERM – often will look very different from another's.

The Business Value Chain

Axis – 3 of the COSO Cube depicting the ERM framework caters for the ***Entity and its Units*** which contribute to the various business activities involved in its operational, tactical and strategic levels. To successfully apply ERM, an entity must consider its entire scope of activities. COSO Cube considers activities at all levels of the organization:

- **Enterprise-level**
- **Division or subsidiary**
- **Business unit processes**

The above three units are also referred as *Business Value Chain* in the industry by Management Consultants.

COSO acknowledges that while the enterprise risk management framework is relevant and applicable to all entities, the manner in which management applies enterprise risk

management will vary widely with the nature of the entity and depends on a number of entity-specific factors. These factors include the entity's business model, risk profile, ownership structure, operating environment, size, complexity, industry and degree of regulation, among others. As it considers the entity's specific situation, management will make a series of choices regarding the complexity of processes and methodologies deployed to apply the enterprise risk management framework components. Management may choose to pursue sophisticated methods and techniques in certain business units or processes or enterprise risk management components, but decide to utilize a more basic approach for others.

2.3 Sophistication of the COSO ERM framework

The sophistication of the COSO ERM framework is due to its ***relationship, and interaction within the three axes***. There is a direct relationship between objectives, which are what an entity strives to achieve, and the enterprise risk management components, which represent what is needed to achieve them.

Each component row cuts across and applies to all four objectives categories. Looking at the objectives categories, all eight components are relevant to each. Taking one category, effectiveness and efficiency of operations, for example, all eight components are applicable and important to its achievement.

ERM is relevant to an entire enterprise or to an individual business unit. This relationship is depicted by the third dimension, which represents subsidiaries, divisions and other business units. The COSO definition reflects certain fundamental concepts critical to any entity. Enterprise risk management:

- *Is a **process** – it's a means to an end, not an end in itself.*

  ERM is not a go – no go static procedure but a more flexible arrangement (Moeller, 2007). ERM is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive and inherent in the way management runs the business. ERM is different from the perspective of

some observers who view it as something added on to an entity's activities, or as a necessary burden. That is not to say effective enterprise risk management does not require incremental effort. For instance, risk assessment may require incremental effort to develop needed models and make necessary analysis and calculations. However, these and other enterprise risk management mechanisms are intertwined with an entity's operating activities and exist for fundamental business reasons.

- *Is **effected by people** – it's not merely policies, surveys and forms, but involves people at every level of an organization.*

  ERM process must be managed by people who are close enough to that risk situation to understand the various factors surrounding that risk, including its implications (Moeller, 2007). An organization's people include the board of directors, as well as management and other personnel. Although directors primarily provide oversight, they also provide direction and approve strategy and certain transactions and policies. As such, boards of directors are an important element of enterprise risk management.

- *Is **applied in strategy setting**.*

  An entity establishes a strategy for achieving its strategic objectives. It also sets related objectives it wants to achieve, flowing from the strategy, cascading to business units, divisions and processes. In setting strategy, management considers risks relative to alternative strategies. Every entity is constantly faced with alternative strategies regarding a vast range of potential future actions. An ERM should play a major role in helping to establish those alternative strategies (Moeller, 2007). Since many organizations are large, with many varied operating units, ERM should be applied across that entire organization, using a portfolio type of approach that blends a mix of its high-and low- risk activities.

- *Is **applied across the enterprise**, at every level and unit, and includes taking an entity-level portfolio view of risks.*

To successfully apply enterprise risk management, an entity must consider its entire scope of activities. Enterprise risk management requires an entity to take a portfolio view of risk.

- *Is designed to identify events potentially affecting the entity and manage risk within its* ***risk appetite.***

  Risk appetite is the amount of risk, on a broad level, that an organization and its individual management are willing to accept in their pursuit of value (Moeller, 2007). Risk appetite is directly related to an entity's strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity's risk appetite. Different strategies will expose the entity to different risks. ERM, applied in strategy setting, helps management select a strategy consistent with the entity's risk appetite.

- *Provides* ***reasonable assurance*** *to an entity's management and board.*

  ERM provides only reasonable assurance, not positive assurance on objective achievements (Moeller, 2007). A well-controlled organization, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period, even for multiple years. However, limitations also result from the realities that human judgment in decision making can be faulty, decisions on risk responses and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions.

- *Is geared to the* ***achievement of objectives*** *in one or more separate but overlapping categories.*

  An organization, through its management, should work to establish high level common objectives that can be shared by all the stakeholders (Moeller, 2007).

COSO ERM definition is purposefully broad for several reasons. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across different types of organizations, industries and sectors. It focuses directly on achievement of entity objectives. And, the definition provides a basis for defining enterprise risk management effectiveness.

According to COSO, while enterprise risk management is a process, its effectiveness is a state or condition at a point in time. Determining whether enterprise risk management is effective is a subjective judgment resulting from an assessment of whether all eight components are present and functioning properly. To be deemed effective, all eight components must be present and functioning. However, this does not mean that each component should function identically, or even at the same level, in different entities, and trade-offs may exist between components. Because enterprise risk management techniques can serve a variety of purposes, techniques applied relative to one component can serve the purpose of those that normally might be present in another. Additionally, risk responses can differ in the degree to which they address a particular risk, so that complementary risk responses, each with limited effect, together may be satisfactory.

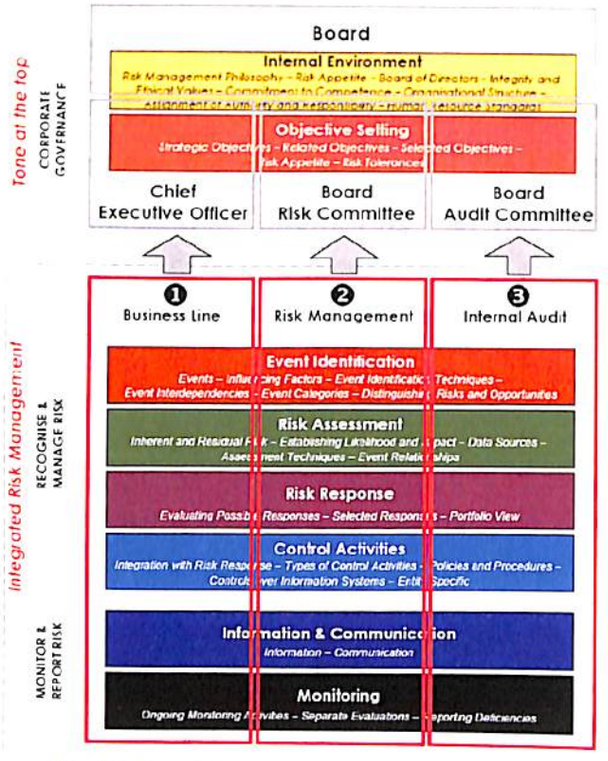

Fig. 2.3 Three Lines of Defence (Rittenberg, 2007)

Three lines of defence approach to ERM

Rittenberg (2007) states that increasingly, organizations are adopting a three lines of defence approach to ERM, embedding risk management capability across the organization. The model distinguishes between functions owning and managing risks, functions

overseeing risks and functions providing independent assurance, all playing an important function within the integrated ERM, as illustrated in Fig. 2.3.

(A) The Board sets the organization's risk appetite, approves the strategy for managing risk and is ultimately responsible for the organization's system of internal control. The Chief Executive, supported by senior management, has overall responsibility for the management of risks facing the organization. Business management and staff have the primary responsibility for managing risk. They are required to take responsibility for the identification, assessment, and management, monitoring and reporting of enterprise risks arising within their respective businesses. Unit, line, and product managers consistently use the chosen ERM framework where all decisions pro-actively consider risk, thereby ensuring an informed risk and reward balance.

(B) The Chief Risk Officer (CRO), supported by the risk functions within the organization, has overall responsibility for the second line of defence. The CRO is accountable to the board risk committee and ultimately to the main board. Day-to-day management of risks is not the accountability of the CRO, but rests with the first line of defence. Typically the risk function recommends risk policies to the board for approval, and oversees the effectiveness of the ERM framework in the identification, assessment, and management, monitoring and reporting of risks. The draft document should also make reference to the Board Risk Committee. The evolving risk-based, principles-driven regulatory landscape, such as the Based II Capital Accord is raising the profile and responsibilities of the Board Risk Committee. COSO has a major opportunity to be the main ERM framework for the evolving risk-based, principles-driven regulation.

(C) The third line of defence – Internal Audit - provides independent assurance on the effectiveness of the first and second lines of defence in the management of enterprise risks across the organization. The Internal Audit function is accountable to the board audit committee and ultimately to the main board. Recent surveys show the internal audit function becoming more standardized throughout the world and is predicted to expand its role in organizational governance and risk management.

2.4 Key elements in Risk Component

Psica (2008) precisely states that, 'an ERM framework is not a single policy, but an array of components within an organization that work together to manage risk over time efficiently and effectively. The salient features comprising the key elements in the COSO Risk Components are studied as these key elements contribute to decision making. They are further deliberated in various studies by McNamee (2004) and Miccolis (2001). Roth & Espersen (2004) acknowledge David McNamee as one of the internal audit profession's thought leaders on risk management. Recent studies focused on the COSO ERM framework with relevance to the general industry practices has been accomplished by Moeller (2007). Walker & Shenkir (2006, 2007), various commentaries from Kloman (2005), Beasley *et al* (2006, 2004). These studies form a watershed of thinking about ERM.

Internal environment

According to COSO ERM (2004), the entity's internal environment is the foundation for all other components of ERM, providing discipline and structure. The internal environment influences how strategies **(PETRO-STRATEGIES)** and objectives are established, business activities are structured and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities. Each of these is shaped according to the entity's culture, history and environment (McNamee, 2004). Internal environment comprises many elements, including an entity's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility. A board of directors is a critical part of the internal environment and significantly influences other internal environment elements. Although all elements are important, the extent to which each is addressed will vary with the entity.

- **Risk Management Philosophy**

  According to COSO ERM (2004), the philosophy comprises of the entity's beliefs about risk and how it chooses to conduct its activities and deal with risks. It

reflects the value the entity seeks from enterprise risk management and influences how ERM components are applied. Management's ERM philosophy is reflected in its policy statements and other communications. McNamee's (2004) admonition through previous findings is through the many reports that in particular point to risk management failure due to a widespread ***lack of imagination*** at top level management. He adds that entities need to break out of current thinking patterns to think broadly about risks.

- **Risk Appetite**

  According to COSO ERM (2004), Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. Entities often consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk. Risk appetite is directly related to an entity's strategy.

- **Risk Culture**

  According to COSO ERM (2004), Risk culture is the set of shared attitudes, values and practices that characterize how an entity considers risk in its day-to-day activities. Management considers how its risk culture affects and aligns with other elements of ERM.

- **Board of Directors**

  According to COSO ERM (2004), an entity's board of directors is a critical part of the internal environment and significantly influences other internal environment elements. The board's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Members of top management may be effective board members, bringing knowledge of the company to the table. But there must be a sufficient number of independent outside directors not only to provide sound advice, counsel and direction, but also to serve as a

necessary check and balance on management. For the internal environment to be effective, the board must have at least a majority of independent outside directors.

- **Evaluating the Corporate Board**

  Allen, Renner & English (2004), have studied about evaluating the Corporate Board which has come into prominence due to mounting pressure to improve Corporate Governance results in the form of new scorecards. Most experts have attributed corporate disasters due to weaknesses in policies, accounting failures and individuals especially company boards which finally distill down to weakness in corporate governance. In line with this, conscientious boards want to benchmark their companies' corporate governance against their peers. To that end, scorecards or yardsticks are available that evaluate boards and offer a benchmark for rating and comparing boards of directors and their practices.

  Apart from the above mentioned internal driver, further pressure to evaluate the board comes from the companies that provide liability insurance to the directors and officers of corporations, as an external driver. For several reasons, insurers have under-funded director and officer (D&O) policies, so, in order to correct this problem, the insuring companies have dramatically increased the prices of D&O insurance premiums. In fact, many large companies have seen their premiums increase by 200% to 400%.

  Four rating agencies provide metrics that rank the quality of an entity's directors. They are Institutional Shareholder Services (ISS), Standard & Poor's (S&P), Governance Metrics International (GMI), and The Corporate Library (TCL).

  In the Wall Street Journal, Langley (2003) has stated that ISS caries the most clout. These rating system providers ***use a number of variables and categories*** to arrive at their indices. Variables range from 61 to 6000 while some have not disclosed them; while categories range from 4 to 8 within these rating providers. Interestingly, the cost of annual subscription ranges from $ 10,000 to $ 80,000 per

annum for obtaining the ratings. According to Sonnenfeld (2004) from the Yale School of Management, "The ratings services evaluate the corporate governance of firms by mixing together empirically based standards and the ***myths and clichés of The Street.***" Using evaluation standards based on Wall Street superstitions rather than research, potential conflicts of interest, and providing ratings don't work. Langley (2003) in her commentaries also notes that the rating services appear to have a conflict of interest.

(A) As companies must pay to discover how they were scored, so they learn how to change their scores. Scorecards can ***appear to be a type of bribery*** when, by paying, companies find out how to improve their scores. The rating service then charges the investors fees for the scores, which results in the ***appearance of lack of independence.***

(B) The ***subscribing company is often the one that must find any errors in the grading***, which may result in costly and time-consuming use of company resources. One concern is whether the rating service or corporation being rated verifies the data. In many cases, a corporation's accountants and financial analysts will be the ones to review the data ***and provide the necessary corrections.***

(C) One final disadvantage is that simply improving ***the score doesn't mean the board actually performs better within closed meetings.*** Good corporate governance may be used to prevent business failures, but investors and others are really interested in success, so the ultimate issue is whether the corporation can make the leap from good corporate governance to good financial performance.

Allen, Renner & English (2004), on the other hand state that the corporate scorecard may be worth purchasing for several reasons.

a) First, a company can ***track improvements in its own governance practices.***

b) Second, board scorecards give companies another ***way to compete by adopting better standards of performance***, which becomes a motivator for change and may ***demonstrate evidence of change at the higher echelons.***

c) Third, high ratings will provide an ***additional marketing tool for investor relations*** departments.

d) Fourth, ***Board Scorecards are superior to SOX and SEC requirements*** for directors. These requirements only focus on the independence and Audit Committee supervision of the external auditor; whereas board scorecards criteria are much broader and incorporate other aspects of board performance, financial results, executive compensation, financial transparency, information disclosure, reputation risks, socially responsible investment issues, evaluation of take over practices, including director's educational credentials.

e) Fifth, fulfilling SOX and stock exchange requirements is in keeping with the ***letter of the law***, scoreboard ratings services appear to be increasing the stakes. Companies that earn higher ratings may, in fact, be responding to the ***spirit of the law***, particularly for proactive companies.

- **Integrity and Ethical Values**

  According to COSO ERM (2004), an entity's strategy and objectives and the way they are implemented and achieved are based on preferences, value judgments and management styles. Management's integrity and commitment to ethical values influence these preferences and value judgments, which are translated into standards of behavior. Management integrity is a prerequisite for ethical behavior in all aspects of an entity's activities. Top management, starting with the CEO plays a key role in determining the corporate culture.

  Integrity and ethical values are essential elements of the environment, affecting the design, administration and monitoring of other enterprise risk management components. Ethical behavior and management integrity are by-products of the corporate culture, which encompasses ethical and behavioral standards and how they are communicated and reinforced.

- **Commitment to Competence**

  According to COSO ERM (2004), Competence reflects the knowledge and skills needed to perform assigned tasks. Management decides how well these tasks need to be accomplished weighing the entity's strategy and objectives against plans for strategy implementation and achievement of the objectives. A trade-off often exists between competence and cost.

- **Management's Philosophy and Operating Style**

  According to COSO ERM (2004), Management's philosophy and operating style affect the way the enterprise is managed, including the kinds of risks accepted. A formally managed entity will rely more on written policies, standards of behavior, performance indicators and exception reports.

  Other elements of management's philosophy and operating style include preference for conservative or aggressive accounting principles, conscientiousness and conservatism with which accounting estimates are developed and attitudes toward financial reporting, information technology, business processes and personnel. The attitude and daily operating style of top management affect the extent to which actions are aligned with risk philosophy and appetite. An effective environment encourages people to pursue business opportunities that align with the entity's risk appetite.

- **Assignment of Authority and Responsibility**

  According to COSO ERM (2004), Assignment of authority and responsibility involves the degree to which individuals and teams are authorized (delegation) and encouraged to use initiative to address issues and solve problems, as well as limits to their authority. The internal environment is greatly influenced by the extent to which individuals recognize that they will be held accountable.

  Sobel & Reding (2004) have studied on aligning Corporate Governance & ERM. They state that Corporate governance is a process a board carries out to provide

direction, authority, and oversight of management for the company's stakeholders. Unfortunately, directors, management, internal and external auditors, and risk managers do not understand corporate governance well, especially from a day-today perspective. They sometimes consider it a nebulous topic: It "means different things to different people" (Anderson & Chapman, 2002). They further state that while the board of directors is the owner of the governance process, day-to-day guidance and oversight by the board clearly is not feasible; the board must rely on other parties like executives, managers, and auditors to help it fulfill its governance responsibilities. The melding of ERM with Governance means Directors, Senior management, Internal & External Auditors, and various Risk Owners must work interdependently (Sobel & Reding, 2004).

In their studies, Sobel & Reding (2004) refer the works on Corporate Governance and the Board, done by Institute of Internal Auditors and 2002 PwC report. They state that the Board of Directors is not directly responsible for risk management and that is management's job. The board should, however, assume ultimate responsibility for corporate governance. The board governs on behalf and for the benefit of the company's stakeholders, who include shareholders, employees, customers, suppliers, and others. In contrast to the board of directors, which 'owns' the corporate governance process, management owns the ERM process.

- **Human Resource Policies and Practices**

  According to COSO ERM (2004), Human resource practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating and taking remedial actions send messages to employees regarding expected levels of integrity, ethical behavior and competence.

- **Differences in Environment and Their Implications**

  According to COSO ERM (2004), The internal environment of an entity's autonomous subsidiaries, divisions and other units can vary widely due to

differences in senior operating management's preferences, value judgments and management styles. Since operating units often are managed in different ways, it is unlikely their internal environments will be the same. It is important, therefore, to recognize the effect that varying internal environments can have on other ERM framework components. The impact of an ineffective internal environment could be far-reaching, possibly resulting in financial loss, a tarnished public image or a business failure.

Objective Setting

Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Without clear objectives it is impossible to identify events that might give rise to risks that could impede the accomplishment of a particular strategy or objective—regardless of the scope of the inquiry (Walker & Shenkir, 2007).

- **Strategic Objectives**

  According to COSO ERM (2004), an entity's mission sets out in broad terms what the entity aspires to achieve. Whatever term is used, such as mission, vision, or purpose, it is important that management, with board oversight, explicitly establishes the entity's broad-based reason for being. From this, management sets its strategic objectives, formulates strategy and establishes related objectives for the organization. Strategic objectives are high-level goals, aligned with and supporting the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders. While an entity's mission and strategic objectives are generally stable, its strategy and related objectives are more dynamic and are adjusted for changing internal and external conditions.

- **Related Objectives**

  According to COSO ERM (2004), establishing the right objectives that support and are aligned with the selected strategy, relative to all entity activities, is critical

to success. By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at operational levels, achievement of which will create and preserve value. Each set of objectives is linked to and integrated with more specific objectives that cascade through the organization to sub-objectives established for various activities, such as sales, production and engineering, infrastructure functions etc. By setting objectives at the entity and activity levels, an entity can identify critical success factors. These are key things that must go right if goals are to be attained. By setting objectives, management can identify measurement criteria for performance, with a focus on critical success factors. Despite the diversity of objectives across entities, certain broad categories can be established:

a) Operations Objectives: These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.

b) Reporting Objectives: These pertain to the reliability of reporting. They include internal and external reporting and may involve financial or non-financial information.

c) Compliance Objectives: These pertain to adherence to relevant laws and regulations. They are dependent on external factors, such as environmental regulation, and tend to be similar across all entities in some cases and across an industry in others.

- **Selected Objectives**

According to COSO ERM (2004), as part of enterprise risk management, management ensures that the entity has selected objectives and considered how they support the entity's strategy and mission/vision. Entity objectives also should align with the entity's risk appetite. Misalignment could result in an entity not accepting enough risk to achieve its objectives or, conversely, accepting undue risks.

- **Risk Appetite**

  According to COSO ERM (2004), Risk appetite, established by management and reviewed by the board of directors, is a guidepost in strategy setting. Companies may express risk appetite as the acceptable balance between growth, risk and return, or as risk-adjusted shareholder value-added measures. The entity's risk appetite is reflected in entity strategy, which in turn guides resource allocation. Management allocates resources across business units with consideration of the entity's risk appetite and individual business units' strategic plans to generate a desired return on invested resources. Management looks to align the organization, people, processes and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.

- **Risk Tolerances**

  According to COSO ERM (2004), Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Event identification

A variety of internal and external factors give rise to events. When identifying potential events, management considers the full scope of the organization. In the risk identification process, those involved should recognize that it is a misperception to think of a risk 'as a sudden event' (Corporate Board Member, 2006).

- **Events**

  According to COSO ERM (2004), An event is an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives. Events may have positive or negative impacts, or both. As part of event identification, management recognizes that uncertainties exist, but does not know when an event may occur, or its outcome

should it occur. Management initially considers a range of potential events, affected by both internal and external factors, without necessarily focusing on whether the potential impact is positive or negative. Potential events range from the obvious to the obscure, and the potential effects from the significant to the insignificant.

Walker & Shenkir (2007) suggest some techniques for identifying risk are: Brainstorming, Event inventories and loss event data, Interviews and self-assessment, Facilitated workshops, SWOT analysis, Risk questionnaires and risk surveys, Scenario analysis, Using technology, Other techniques. Under other techniques, possible approaches for identifying risks include ***value chain analysis***, system design review, process analysis, and benchmarking with other similar as well as dissimilar organizations. Also, external consultants can add value in the risk identification process by bringing in knowledge from other companies and industries and by challenging the company's list of identified risks.

Most Management Consultants invariably use a proprietary *Value Chain Model* and analysis in the oil industry.

- **Factors Influencing Strategy and Objectives**

  According to COSO ERM (2004), a myriad of external and internal factors influences how events could potentially affect strategy implementation and achievement of objectives. As part of enterprise risk management, personnel recognize the importance of understanding external and internal factors and the type of events that can emanate there from. Management considers current factors, as well as those that may occur in the future.

- **Event Identification Methodology and Techniques**

  According to COSO ERM (2004), an entity's event identification methodology may comprise a combination of techniques, together with supporting tools. Event

identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, changes in commodity prices and lost time accidents. Techniques that focus on future exposures consider such matters as exposure to shifting demographics, new market conditions and competitor actions, scenario planning. Techniques vary widely in level of sophistication. Many of the more sophisticated techniques are industry-specific, where many Management Consultants have a niche market, with proprietary methodology.

- **Event Interdependencies**

  According to COSO ERM (2004), events do not occur in isolation. One event can trigger another, and events can occur concurrently. In event identification, management should understand how events interrelate. By assessing the interrelationships, one can determine where risk management efforts are best directed.

- **Event Categories**

  According to COSO ERM (2004), it may be useful to group potential events into categories. Event categorization also allows management to consider the completeness of its event identification efforts. Furthermore, event categorization can reinforce an entity-level portfolio view of events across the entity.

- **Distinguishing Risks and Opportunities**

  According to COSO ERM (2004), events may have a negative impact, a positive impact or both. Events with a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is the possibility that an event will occur and adversely affect the achievement of objectives. Events with a potentially positive impact represent opportunities, or offset the negative impact of risks. Events representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Events potentially offsetting

the negative impact of risks are considered in management's risk assessment and response. Walker & Shenkir (2007) caution that the point is to understand the level at which quantification can best occur. If the risk is quantified at too high a level, it could be too broad or not actionable. Using a ***building block approach around risk drivers*** facilitates the quantification process. At the end of the process, however, quantification is still an estimate and should be viewed as merely providing an ***order of magnitude*** of the impact.

Risk assessment

Although the internal and external factors are common to companies in an industry, many are unique to a particular entity, because of its established objectives and past choices. McNamee (2004) also adds that a risk model can show current exposures, but a truly useful model also will show possible future exposures. He recommends that a risk model for assessment and implementation is best created by the organization with outsiders used as resources for training and validating the framework. Walker & Shenkir (2007) argue that once risks are identified, some organizations find it helpful to categorize them. This may be a necessity if the risk identification process produces hundreds of risks (like in the oil & gas industry), which can be overwhelming and seem unmanageable. Risk categories include hazard, operational, financial, strategic, and compliance. Other categories exist as are controllable or non-controllable and external or internal. Categorizing risk requires an internal risk language or vocabulary that is common or unique to the organization in total, not just to a particular subunit or silo. Studies have shown that an inconsistent language defining risks across an organization is an impediment to an effective ERM strategy. Risk terms would certainly vary between a pharmaceutical company and a technology company or between a nonprofit and an energy company.

- **Inherent and Residual Risk**

  Management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the

risk's likelihood or impact. Residual risk is the risk that remains after management responds to the risk. Understanding residual risk can provide major benefits because companies do not want to over or under-manage a risk that may be deemed by management and stakeholders to be 'tolerable' or 'acceptable' relative to stated business objectives. This is a major reason why some companies adopt ERM and try to understand, even qualitatively, the return on investment (ROI) of an ERM program (Walker & Shenkir, 2007).

- **Estimating Likelihood and Impact**

  According to COSO ERM (2004), uncertainty of potential events is evaluated from two perspectives i.e., likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect. Determining how much attention should be given to assessing the array of risks an entity faces is difficult and challenging. Management recognizes that a risk with a low likelihood of occurrence and little potential impact generally does not warrant further consideration. On the other hand, a risk with high likelihood of occurrence and significant potential impact demands considerable attention. Circumstances in between these extremes usually require difficult judgments. Because risks are assessed in the context of an entity's strategy and objectives, management naturally tends to focus on risks with short- to mid-term time horizons. However, some elements of strategic direction and objectives extend to the longer term. As a result, management needs to be cognizant of the longer timeframes, and not ignore risks that might be further out.

  McNamee (2004) remarks that, the challenge in estimating is to treat low probability events that might have a major negative outcome. In contrast to the usual perception, he further argues that the use of a probability equation in risk management is a technique leftover from insurance risk management practice. He states that, 'When thinking about the unthinkable, probabilities make no sense. I argue that probability should have little or no bearing on the decision to manage

the risk, but probability has a significant bearing on the methods chosen to manage the risk.'

- **Qualitative and Quantitative Methodology and Techniques**

  According to COSO ERM (2004), an entity's risk assessment methodology comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data is not cost-effective. Quantitative assessment techniques usually require a higher degree of effort and rigor, sometimes using mathematical models. Quantitative techniques are dependent on the quality of the supporting data and assumptions, and are most relevant for exposures that have a known history and frequency of variability and allow reliable forecasting. A summary of various Qualitative & Quantitative Approaches to Risk Assessment is shown in Fig. 2.4.

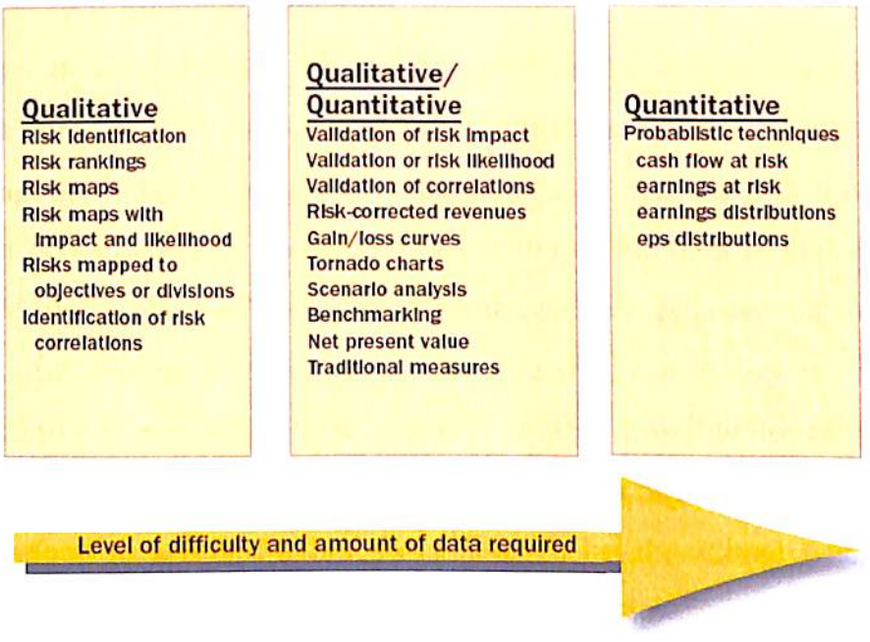

Fig. 2.4, 'Qualitative and Quantitative Approaches to Risk Assessment'
(Source: Statements on Management Accounting, IMA, 2007)

Risk is viewed as an objective phenomenon and is quantifiable in branches of mathematics based on certain assumptions, parameters and formula which takes a deterministic approach. Risk is viewed as a subjective phenomenon which may

not be accurately quantifiable in branches of social sciences – economics, psychology, sociology etc. Objectivity is the main tool of technical managers, engineers etc. but subjectivity affects operational managers in the face of uncertainty. Some scholars who subscribe to this subjective approach argue that if the future is either predetermined or independent of present human activities then the term risk does not make any sense (Renn, 1992). From this perspective the understanding of risk is fluid and most of the work on risk in the social sciences does not target any rigid objective. Consequently, a broader picture of risk emerges in the social sciences than that focused on by many mathematicians (Zinn, 2006). However at a practioner's level, risk is viewed from both perspectives (Skipper, 2005).

Walker & Shenkir (2007) have suggested the following methods based on their various studies in different organizations.

(A) *Risk Rankings* - ERM team prioritize the risks on a scale of importance, such as low, moderate, and high.

(B) *Impact & Probability* - ERM team generate Risk Maps using impact and probability. In ERM implementation, companies not only generate risk maps to capture impact and likelihood but also to demonstrate how risks look when put together in one place. The value of the map is that it reflects the collective wisdom of the parties involved. Furthermore, risk maps capture considerable risk information in one place that is easily reviewed. When qualitatively assessing these risks, it is also possible to estimate ranges. Studies have shown that Risk maps can help an organization determine how to respond to a risk. Several keys need to be considered when generating risk maps: confidentiality, definitions, timeframe, direction, and correlations. One weakness in risk maps (and in silo risk management) is that maps do not capture any risk correlations. Ignoring risk correlations can lead to ineffective and inefficient risk management.

(C) *Tornado charts* - A gain/loss curves that attempt to capture how much of an impact a risk has on a particular metric such as revenue, net income, or

earnings per share. Tornado charts do not show correlations or distributions, but they are valuable because executives can see, in one place, the biggest risks in terms of a single performance metric.

(D) *Risk-Adjusted measures* – A risk corrected measure to see how revenues would look if risks were managed better.

(E) *Common Sense Approach to Risk Assessment* – They argue that some of these risk metrics and tools are difficult; a simple approach can yield equally good results. One approach is to measure where the company stands today on a risk issue. After implementing risk mitigation techniques, the company can reassess the risk issue. They also acknowledge that, 'of course, not all of the improvement related to a risk can be traced to the risk mitigation techniques, but improvement is still valuable.'

(F) *Probabilistic Models* - Some organizations use quantitative approaches in ERM that are built on traditional statistical and probabilistic models and techniques. The disadvantage to these approaches is that they require more time, data, and analysis and are built on various assumptions. Furthermore, using the past to predict the future has limitations even before other *explanatory variables* are included in the statistical prediction process. But some organizations still find these models very useful as a tool in their solutions toolkit when approaching risk.

(G) *Non-quantifiable risks* - Some risks seem to defy acceptable quantification, but a deeper look can reveal valuable information. Reputation is a risk that as become increasingly important in today's business environment, and it must be managed. At first glance, some executives would say you cannot quantify it, but it can be in some ways. In academia, a university's reputation is a prodigious risk. For public companies, decreases in stock prices surrounding an event that damaged an organization's reputation are a phenomenal risk. Similar risk would be a breach in IT security.

Risk response

In considering risk response, management considers costs and benefits, and selects a response that brings expected likelihood and impact within the desired risk tolerances. '***ERM is highly strategic in nature***' (Ward, 2006); She further states that by having an overarching enterprise-wide view of how and where risks are mitigated and opportunities exploited, decision-making is enhanced through a higher visibility of risk exposure and the acceptance or exploitation of risk on an informed basis. Moreover, a high degree of risk awareness at the strategic level builds resilience to external shocks and agility in responding to adversity and opportunity. Importantly, ERM is more than just tools and a technique. ERM is a discipline and an embedded philosophy that drives a continuous process of improved decision-making, efficiency, and performance.

- **Identifying Risk Responses**

  According to COSO ERM (2004), Risk responses fall within the following categories:

  a) Avoidance – Action is taken to exit the activities giving rise to risk.
  b) Reduction – Action is taken to reduce the risk likelihood or impact, or both.
  c) Sharing – Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk.
  d) Acceptance – No action is taken to affect likelihood or impact.

- **Assessing the Costs Versus Benefits**

  According to COSO ERM (2004), In determining potential responses, management should consider such things as:

  a) Evaluating effects of potential risk responses on risk likelihood and impact – and which response options align with the entity's risk tolerances,
  b) Assessing the costs versus benefits of potential risk responses, and
  c) Possible opportunities to achieve entity objectives going beyond dealing with the specific risk.

Once management selects a response, it may need to develop an implementation plan to execute the response and recalibrate the risk on a residual basis. Additionally, procedures are needed to enable management to ensure effective implementation of the actions. Those procedures represent Control Activities. Management recognizes that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

- **Portfolio View**

  According to COSO ERM (2004), Management considers risk from an entity-wide, or portfolio, perspective. With a view of risk for individual units, the senior management of the enterprise is positioned to take a portfolio view, to determine whether the entity's risk profile is commensurate with its overall risk appetite relative to its objectives. Risk may exist in different units that are within the risk tolerances of the individual units. But taken together, the risk might exceed the risk appetite of the entity as a whole, in which case additional or different risk response is needed. Conversely, risks may naturally offset across the entity, or individual units may be relatively risk averse. Where the portfolio of risk is considerably less than the entity's risk appetite, management may decide to motivate individual business unit managers to accept greater risk in targeted areas to enhance the entity's overall growth and return. In establishing a portfolio view of risk responses, management will recognize the diversity of responses selected and the effect of multiple responses on the entity's risk tolerances.

- **Risk Metrics**

  According to Miccolis et al (2003), ERM clearly links risk management with the creation of organizational value and express risk in terms of impact on organizational objectives. An important aspect of ERM is therefore the strong linkage between measures of risk and measures of overall organizational performance. Industry specific overall performance metrics are therefore used

which then render themselves as for specific application in the risk identification and measurement.

According to the IIA Research Foundation and many publications, ***Value at Risk (VaR)*** and ***Economic Capital (EC)*** are very commonly used risk metrics in most organizations.

VaR was used by J.P. Morgan in the late 80s and 90s for their trading portfolios and has now become popular due to the portfolio approach to risk in the ERM system. EC is a metric popularly used in the Insurance industry whereas Var is embraced in most industries including banking and oil & gas industry.

A Tillinghast Towers Perrin Global Survey (2007) on Insurance sector states that, 65% of Insurers used EC in 2006, which had risen from a 54% use in 2004 (Mueller, 2007).There are pros and cons for both the metrics and many research reports suggest that there is a propensity in the insurance industry to migrate from VaR to EC. Mueller (2007) also states that there is no right or wrong approach to building an EC model for Solvency II implementation; and EC has proven to be an effective metric for quantifying risk in an ERM framework.

Economic Capital (EC) is:

> Market value of assets minus fair value of liabilities and is used in the practice as a risk-adjusted capital measure; specifically, the amount of capital required to meet an explicit solvency constraint (Miccolis et al, 2003).
>
> Measured as the difference in 'market–consistent net assets' between normal conditions and stressed conditions (Mueller, 2007).

Value at Risk (VaR) is:

> The maximum loss an organization can suffer, under normal market conditions, over a given period of time at a given probability level (Miccolis et al, 2003).

Stulz et al (2006) state that additional research is needed to help with the implementation of ERM. There has been much attention for VaR. Correlations between different types of risks are essential in measuring firm-wide risk. Existing research thus far provides little help in estimation and correlation for implementing an ERM system. Firms find some hard to quantify risks to be extremely important. Like Reputation risks or Strategic risks. At this point, there is little research that helps practioners in assessing these risks, but much gain could be made by understanding these risks better even if they cannot be quantified reliably. Notwithstanding the above limitation, implementation of ERM has made a great deal of progress and shareholders have benefited.

Control activities

According to COSO ERM (2004), Control activities occur throughout the organization and include a range of activities.

- **Integration with Risk Response**

  According to COSO ERM (2004), Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which an enterprise strives to achieve its business objectives. In selecting control activities, management considers how they interrelate. An entity might rely on a single control activity to address multiple risk responses. On the other hand, it might be necessary to consider multiple control activities relative to a risk response.

- **Types of Control Activities**

  According to COSO ERM (2004), many different descriptions of types of control activities have been put forth, including preventive controls, detective controls, manual controls, computer controls and management controls.

- **Policies and Procedures**

  According to COSO ERM (2004), Control activities usually involve two elements: a policy establishing what should be done and procedures to effect the policy. A procedure will not be useful if performed mechanically and without a sharp, continuing focus on conditions to which the policy is directed. Further, it is essential that conditions identified as a result of the procedure be investigated and appropriate corrective actions taken.

- **General Controls**

  According to COSO ERM (2004), Information technology-led improvement efforts often help build controls into the operations of an organization. Such initiatives may include business process improvement, total quality management and defect identification and management.

- **Application Controls**

  According to COSO ERM (2004), Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and processing.

- **Entity Specific**

  According to COSO ERM (2004), because each entity has its own set of objectives and implementation approaches, there will be differences in risk responses and related control activities. Even if two entities had identical objectives and made similar decisions on how they should be achieved, their control activities would likely be different. Each entity is managed by different people who use individual judgments in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well

as the complexity of its organization, its history and its culture. The environment in which an entity operates affects the risks to which it is exposed and may present unique reporting objectives or special legal or regulatory requirements. Other factors that influence an entity's complexity and therefore the nature of its controls include location and geographical dispersion, the extensiveness and sophistication of operations, and information processing methods. All these factors affect an entity's control activities, which need to be designed accordingly to contribute to the achievement of the entity's objectives.

Information and communication

- **Information**

  According to COSO ERM (2004), Information is needed at all levels of an organization to identify, assess and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources – internal and external, and in quantitative and qualitative forms – and facilitates responses to changing conditions. The challenge for management is to process and refine large volumes of data into actionable information. Keeping information consistent with needs is particularly important when an entity faces fundamental industry changes, highly innovative and quick-moving competitors, or significant customer demand shifts. Information systems must not only identify and capture needed financial and non-financial information, they must also process and report this information in a timeframe and way that are useful in controlling the entity's activities. Information System should also ensure data quality to enable effective decision making.

- **Communication**

  Information systems must provide information to appropriate personnel so that they can carry out their operating, financial reporting and compliance responsibilities. McNamee (2004) states that a method for regularly

communicating and sharing what is accumulated as an information, including a common risk language is important for successful risk management. He also acknowledges that this is culture-specific and best developed by people with in-depth knowledge of the organization and its communication-response patterns. While Mulligan *et al* (1998) state that 'An effective risk communication policy includes commitments to: open and honest communication; early release of information; meaningful processes for explaining risks; processes for incorporating community concerns and values; shared decision-making; and a relationship built on trust.'

Monitoring

According to COSO ERM (2004), An entity's enterprise risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change. In the face of such changes, management needs to determine whether the functioning of each enterprise risk management component continues to be effective.

- **Ongoing Monitoring Activities**

  Many activities serve to monitor the effectiveness of enterprise risk management in the ordinary course of running the business.

- **Separate Evaluations**

  According to COSO ERM (2004), while ongoing monitoring procedures usually provide important feedback on the effectiveness of other enterprise risk management components, it may be useful to take a fresh look from time to time, focusing directly on enterprise risk management effectiveness. This also provides an opportunity to consider the continued effectiveness of the ongoing monitoring procedures. Internal auditors normally perform evaluations as part of their regular duties, or at the specific request of senior management, the board or subsidiary or divisional executives. Similarly, management may utilize input from external

auditors in considering the effectiveness of enterprise risk management. A combination of efforts may be used in conducting whatever evaluative procedures management deems necessary.

Psica (2008), states that because internal audit resources are usually targeted to the areas of highest risk, it is essential that the ERM framework is audited periodically to ensure that it has the capacity to identify the right risks to produce reliable information on which to base resource allocation, audit planning, and other decisions. She further adds that as convergence drives organizations to find synergies among their audit, compliance, and risk management functions, it is important to provide assurance that the risk management function is sound so that the various parts of the organization can rely on the results of the function. It is an auditor's responsibility to provide an opinion on the audit objective, such as the ***efficiency and effectiveness*** of the framework. According to McNamee (2004), the method chosen to perform internal audit risk assessments and identify areas for risk management should have strong links to the organization's business planning process. There is only one set of business risks, and a big mistake is for internal auditors and the business planning process to independently develop and use models that have not been integrated.

McNamee (2004) further compares the process across other organizations and states the situation is till worse in some organizations as several groups are charged with managing specific risks like information security, health and safety, project risk, etc and each of them have their own developed systems. Internal auditing could be an integrating force to help the organization see that these silos of risk management need to be cross-linked to ensure that an important risk does not get missed. He recommends that the primary step is to get internal auditing represented on the organization's risk management committee so that these issues can be raised and explored. The role of Internal Auditors in an ERM environment has been best summarized by The Institute of Internal Auditor, UK & Ireland as depicted in Fig. 2.5.

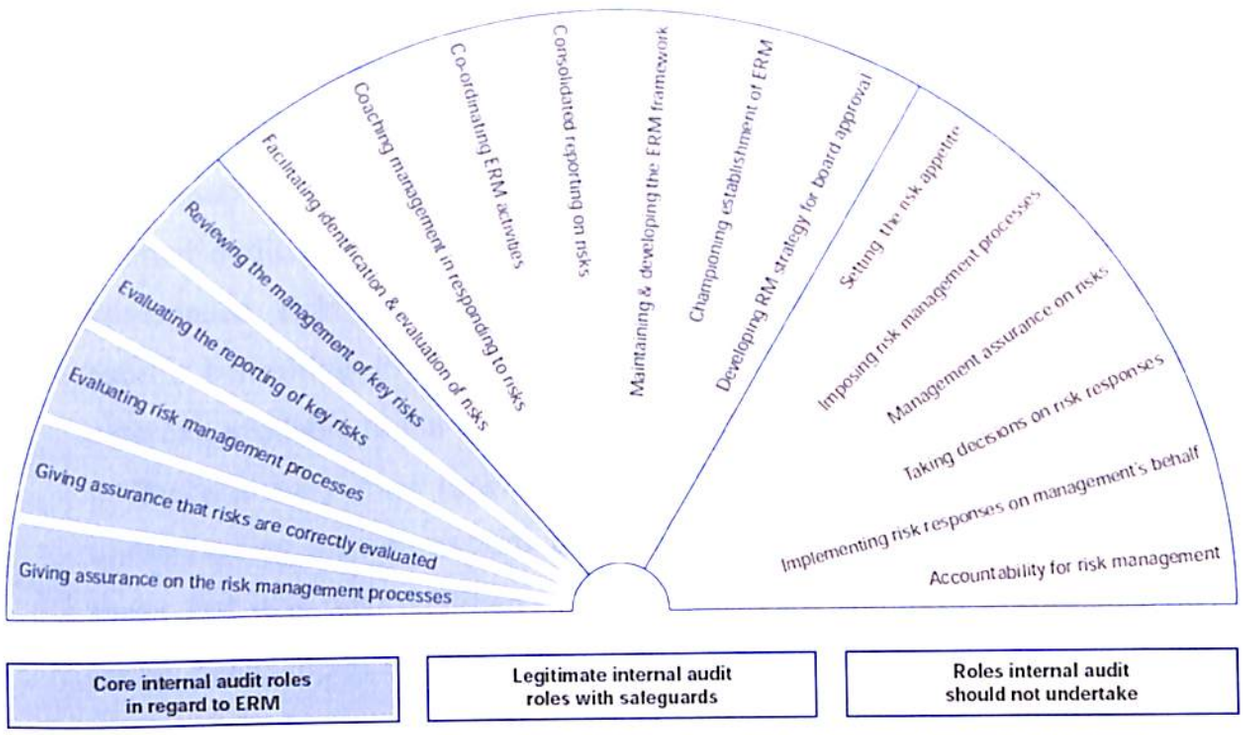

Fig. 2.5, Internal Audit Role in ERM (2004) by the Institute of Internal Auditor, UK & Ireland

The Institute of Internal Auditors (UK & Ireland) state that, 'Internal auditing is an independent, objective assurance and consulting activity.' Its core role with regard to ERM is to provide objective assurance to the board of directors on the effectiveness of risk management.

Research by Deloitte & Touche (2003) has shown that board directors and internal auditors agree that the two most important ways that internal audit provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively. Figure 7 presents a range of ERM activities and indicates which roles an effective professional internal audit function should and, equally importantly, should not undertake. The key factors to take into account when determining internal audit's role are whether the activity raises any threats to the internal audit function's independence and objectivity and whether it is likely to improve the organization's risk management, control and governance processes.

The activities on the left of Figure 7 are all assurance activities. They form part of the wider objective of giving assurance on risk management. An internal audit function complying with the International Standards for the Professional Practice of Internal Auditing can and should perform at least some of these activities. Internal audit may provide consulting services that improve an organization's governance, risk management, and control processes. The extent of internal audit's consulting in ERM will depend on the other resources, internal and external, available to the board and on the risk maturity of the organization and it is likely to vary over time. Internal audit's expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that it is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction. As the organization's risk maturity increases and risk management becomes more embedded in the operations of the business, internal audit's role in championing ERM may reduce. Similarly, if an organization employs the services of a risk management specialist or function, internal audit is more likely to give value by concentrating on its assurance role, than by undertaking the more consulting activities. However, if internal audit has not yet adopted the risk-based approach represented by the assurance activities on the left of Figure 7, it is unlikely to be equipped to undertake the consulting activities in the centre.

- **Reporting Deficiencies**

  According to COSO ERM (2004), deficiencies in an entity's enterprise risk management may surface from many sources, including the entity's ongoing monitoring procedures, separate evaluations and external parties. The term *deficiency* refers to a condition within the enterprise risk management process worthy of attention.

  While dealing with reporting of deficiencies, IIA (UK & Ireland) explains its viewpoint through one of its position policy statements, on the consultative role of Internal Auditors (IIA Position Statement, 2003). Referring back to Fig 7, the

centre of figure shows the consulting roles that internal audit may undertake in relation to ERM. In general the further to the right of the dial that internal audit ventures, the greater are the safeguards that are required to ensure that its independence and objectivity are maintained. Some of the consulting roles that internal audit may undertake are:

(A) Making available to management tools and techniques used by internal audit to analyze risks and controls.

(B) Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization.

(C) Providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding.

(D) Acting as the central point for coordinating, monitoring and reporting on risks.

(E) Supporting managers as they work to identify the best way to mitigate a risk.

The key factor in deciding whether consulting services are compatible with the assurance role is to determine whether the internal auditor is assuming any management responsibility. In the case of ERM, internal audit can provide consulting services so long as it has no role in actually managing risks, that is management's responsibility, and so long as senior management actively endorses and supports ERM.

2.5 Key elements in Risk Universe

Ballou & Heitger (2005) and other publications note that entities now face unprecedented challenges as they compete in an increasingly global, volatile, and regulated business environment. Furthermore, meeting customer needs, managing complex supply chains, utilizing strategic alliance partners, and ensuring effective and efficient internal business

process performance are increasingly more difficult, even with today's more sophisticated, real-time information systems. Added to these pressures are the threats to an organization's reputation. There is an ever strengthening public perception that organizations are improperly, or not all, socially responsible. This perception is due in part to the public's belief that organizations are not doing enough to improve the communities and environments in which they operate. Further damaging organizations' reputations are the distrust from various frauds and reporting restatements. Taken together, the increasingly complex nature of business risks suggests that entities need to develop a formal process for managing their portfolio of risk properly and appreciate the practical challenges in the Risk Universe, before the risk management process can reach its potential.

Risk dimensions

Oil & gas companies constitute some of the world's largest corporations. Such size and scale introduces additional challenges in managing risks. Commentaries from The Institute of Internal Auditors acknowledge that, ***the consolidated reporting of disparate risks*** in the COSO ERM framework (2004) are achieved by classifying risks into Strategic, Operational, Compliance and Financial categories in the COSO Cube. Miccolis et al (2003), Meulbroek (2002) including various authors cite some of the risks in the risk universe that an entity normally gets exposed as follows.

- ***Strategic risks*** include merger and acquisition integration problems, competitive pressure, research and development delays, customer demand shortfall, customer pricing pressure, loss of major customers and regulatory problems. Walker and Shenkir (2006) have included political, economic, regulatory, and global market conditions; including reputation risk, leadership risk, brand risk, and changing customer needs.

- ***Operational risks*** include management ineffectiveness, system failures, accounting irregularities, product design and manufacturing defects, cost over runs and supply chain problems. Walker and Shenkir (2006) have included in

their studies technology, business continuity, environment, health and safety (EHS), product/service failure, efficiency, capacity and change integration. According to Marie & Rao (2007), unlike financial risks, ***operational risks mostly arise due to factors that are internal to the organization***. Operational risks are managed through changes in processes, technology, people, organizations, and culture—not through hedging in the financial markets. Managers need a risk modeling approach that provides them with information on how the operational risk would change if they were to implement alternative operational decisions. Operational risks can be loosely classified into event risks and business risks. Event risks refer to isolated occurrences that generate losses such as technology failure, fraud, etc. Business risks are created by business decisions like changes in distribution strategy, launching a new product, etc. (Berlin, 2004).

- ***Compliance risks*** also classified as ***Hazard risks*** (in actuarial studies) include catastrophes and natural disasters, environmental pollution, property risk, product liability and other risks involving lawsuits and compliance requirements. Barton et al (2002) have included impairment of physical assets and terrorism in their studies.

- ***Reporting risks*** or ***Financial risks*** include economic risk, market risk, credit risk, asset-liability risks, interest rate changes, liquidity risk, inflation risk, pension plan funding risks, and global macro economic issues (Berlin, 2004). Marie & Rao (2007) explain that for the most part, ***financial risks originate from outside the organization and are beyond a firm's direct control.*** These include macroeconomic risks, such as interest rates, exchange rates, and asset performance, as well as insurable risks, which include mortality and property/casualty claims. Financial risks are managed through building statistical model distributions representing each of the financial risks and then mathematically combining the distributions.

The classification of risks can be contentious for risk owners depending on the bailiwick where their interests lie. Management Consultants have a great deal of their time expended to tactically allocate the risks derived from their ***risk taxonomy*** to the risk owners along the business value chain. This fact is also highlighted in studies by Miccolis et al (2003), as they acknowledge in their studies that, '***the precise slotting of individual risk factors under each of these four categories is less important than the recognition that ERM covers all categories and all material risk factors that can influence the organization's value.***' Comparative studies by Lewis et al (2005) on the risks faced by oil and gas industry mention that, while certain risks are common across all industries like risks arising in respect of contract management, securities regulations, labour laws, etc., entities in each specific industry face certain risks unique to that industry. Accordingly, ***companies in a particular industry commonly adopt certain customs and practices on an industry-wide basis to allocate those risks in a generally accepted manner.*** This is particularly true in the oil and gas industry, which is ***highly specialized***, ***country-specific*** and composed of a ***relatively small number of key players.***

The flexibility of the risks associated in the Risk Universe is also highlighted in studies done by Marie & Rao (2007). They state that ***some strategic risks could also be financial risks or operational risks***. They state that Strategic risks are risks that can be addressed only through substantial expenditures and/or a change in strategic direction. Many financial risks fall into this category because of the substantial impact they pose. Strategic operational risks can arise, when an organization enters unfamiliar business territory because there is a major acquisition, a new competitor emerges, or customers' buying preferences change, including project risks. Walker & Shenkir (2007) state that, ***generic industry wide portfolio of risks*** is available in various publications and specialist consulting firms. These data base are generally proprietary by nature and highlight the salient risks in the risk universe. A summary of risk type and a definition is presented below:

- *Market Risk*: Change in financial markets affects value of a portfolio

- *Credit Risk*: Change in the credit worthiness of counterparty affects the value of a loan/portfolio. Also counterparty may fail to honor a commitment to make payments
- *Liquidity Risk*: Inability to raise cash, or risk of not being able to execute a transaction at prevailing prices
- *Operational Risk*: Risks arising out of inadequate systems, management failure, human error, fraud, etc.
- *Legal/Regulatory Risk*: Impact due to changes in legal or compliance burdens
- *Business Risk*: Risks due to randomness or uncertainty of product demand, prices, etc.
- *Strategic Risk*: Risk of investments that has high uncertainty of financial success
- *Reputation Risk*: Risks arising out of rumors, scandals, or true corporate mismanagement that results in loss of reputation

Blanco & Regan (2006) state that ***Reputation risk*** and Crisis management is a new frontier in risk management as reputation risk clearly falls into the 'hard to quantify' as well as 'hard to define' categories. They refer to a PwC and Economic Intelligence Unit (EIU) survey report stating that, worldwide, reputational risk was perceived to be the greatest threat. The main reasons behind reputational risk failures are the following:

- The lack of ownership of that risk as it is seen as something that falls outside the mandate of the risk management process.
- Difficulty in measuring the implications of reputational risk events.

Recent energy related examples of reputation risks include the following international cases:

2003: *Occidental Petroleum aiding Columbian Government in bombing, loss US$ 12 Mn.*

2004: *BP manipulations of Propane Market, fined US$ 2.5 Mn. by NYMEX.*

2004: *Royal Dutch Shell's Miscategorization of oil reserves, loss US$ 6 Bn.*

2005: *China Aviation Oil Singapore's Derivatives scandal, loss US$ 50 Mn. (Ling & Lee, 2005).*

2006: *BP Prudhoe Bay, Alaska pipeline Environmental & Health disaster, loss US$ 2 Bn.*

2006: *BP Refinery in Texas - Safety disaster, fine of US$ 21.4 Mn. by Environmental regulators.*

The key to managing reputational risk is prevention. In addition, when prevention is not enough, it is crucial to have contingency plans to break the reputational vicious circle as soon as it starts developing. From a corporate governance perspective, the entity's Board has a fiduciary duty to ensure that a reputational risk management strategy is in place at the firm, and that appropriate resources are dedicated to manage the firm's reputation.

A report by a leading international law firm, Lovells International states that several aspects of the oil and gas industry e.g. the capital-intensive nature of the industry, market price volatility, geographic scope of assets and operations, the high-risk nature of exploration and exploitation of natural resources, technology requirements, environmental concerns, downstream brand promotion and protection issues, political sensitivities, scale and diversity of employee base, give rise to particularly high levels of ***Legal risk*** for international oil and gas companies (Lewis *et al*, 2005). Since a significant amount of oil and gas resources are controlled by national governments, state-owned oil companies are important players in oil and gas projects around the world. While a certain degree of standardization of terms of exploration contracts exists around the world, local governments also can dictate many deal terms. Dealing with state-owned oil companies in various jurisdictions introduces additional risk, complexity and political sensitivity to these transactions.

Lewis *et al*, (2005) further state that the ***oil & gas industry itself is not one of the most heavily regulated industries***, in terms of industry-specific regulations, the operations of oil companies are subject to a wide array of regulations such as environmental, labour, regulations, securities, tax, trade, distribution and transportation. International projects, whether or not involving state-owned oil companies of the host country, can also be subject to foreign investment and other country-specific rules regulations. As such, oil and gas companies devote substantial resources to ensure regulatory compliance. They also pay close attention to the processes involved in the conduct of business (for example,

the processes involved in obtaining and maintaining licenses, in transferring licenses and participations, etc.) and to the impact of changes in applicable legislation. In the oil and gas industry, as in all other industries, range of legal risks arises by ***reference to relationships*** between the company and other players in the market. Governments consider a secure supply of oil and gas products to be a matter of national security.

Lewis *et al* (2005) further state that this lead to ***Political risk.*** While political risk itself is separate and distinct from legal risk or any other risk, they are often connected and have an unquantifiable effect (Berlin, 2004). Similarly, they also note that some legal problems can give rise to political responses. Governments in various parts of the world also apply ***anti-trust laws*** to certain other operational aspects of the oil and gas industry. Regulatory regimes often have somewhat conflicting requirements and procedures regarding notice of acquisitions, pre-clearance of acquisitions, etc. It should be noted that there are both proponents and famous opponents like Allan Greenspan himself. However, as part of the petro-strategy, certain oil companies look to internationalize their operations either to spread risk or to respond to market factors. Therefore, oil & gas companies need to assess the competition law implications not only of mergers and acquisitions but also of pricing arrangements. Political risk management overlaps with almost all ERM components along each of the four objectives categories (DiPiazza Jr & Bremmer, 2006).

While dealing with ***risks due to expropriation of oil & gas assets*** by Governments, parties involved assess risks and evaluate the legal and political recourse thereof. The question of what is fair and equitable treatment often depends on the political atmosphere surrounding an expropriation. Lewis et al (2005) state that, "The experience of international oil companies that had oil and gas related assets expropriated in the last century indicates that the company which has its assets taken in this process is likely to feel that its long term value has been reduced by an amount that exceeds the compensation that is offered by the expropriating government."

Petro-strategies are pursued by major investment projects and undertaken through often a long and complex contracting methodology. The majority of oil and gas projects involves

a series of inter-locking contracts and in many cases may involve external commercial debt financing. As such, contracts in the oil and gas industry require a high level of expertise not only in respect of general international contract drafting and negotiation skills, but also specialized expertise in international oil industry customs and practices as well as specialized areas of international law and practice, environmental law, construction law, real estate law, international commercial finance, transportation and shipping, boundary delimitation issues, host government agreements, international arbitration, consumer protection, etc. This exposes the oil & gas industry again to a range of ***contract & project risks*** which arises by reference to relationships between the company and other players in the market. Dealing with such risks the interdependent relationship does create a framework where ***co-operation rather than adversarial approaches*** is the order of the day.

Global oil market has been extremely volatile and market prices have been subject to a large number of events outside of the control of oil companies. ***Risks from oil fundamentals*** include the drivers from supply demand dislocation (James & Fusaro, 2006).

- Supplies can be limited by such events as labour disputes, civil unrest, court injunctions, terrorist attacks, war, mechanical breakdowns, refinery shut down, an unforeseen change in government policy, extreme weather.
- Demand can be greatly altered by a sudden change of weather, adoption of new technology, change in government policy, terrorist attacks, and speculation.

This historic volatility has also increased the difficulty of managing a variety of ***commercial risks*** arising from contractual obligations. In this context, Wagner (2000) makes a distinction between political risk and commercial risk. He states that, "A political risk is presumably not within the control of the investor, and a commercial risk is."

Day-to-day operations create numerous ***Hazard risks*** for oil & gas companies. Hazard risks include well blowouts in the upstream value chain, fire, explosion in the downstream refinery operations. Some studies have also treated them as part of

operational risk. In actuarial studies hazard risks are also classified under the compliance risks. The basic premise of this classification is that due to non-compliance to regulations set out, the hazard occurs in their studies. However, the liability due to hazards is not unique to the oil and gas sector but the size and scope of operations and the inherent risks in dealing with oil & gas products makes this a more serious concern than in many other sectors. Hydrocarbon extracting, refining, and transporting oil products can all create potential environmental problems leading to ***Environmental risks***. In the West, non-compliance with environmental regulations, with or without accompanying actual environmental damage, generally will result in aggressive responses by environmental protection advocacy groups. Failure to implement appropriate pro-active earth-friendly compliance measures or public relations programs can have a serious negative impact on an oil company's operations and financial results leading to ***Reputational risk***. The impact of the actions of some oil companies upon local populations has recently become a matter of major concern in the industry. The policies and actions of government officials in some resource-rich developing countries may result in ***gross human rights violations***, and to the extent that oil companies are alleged to have facilitated such activities (Lewis *et al* 2005).

Due to extreme volatility of energy commodity prices it has long been considered that businesses operating in the oil & gas sector are particularly susceptible to market (price) risks and other commercial risks. However, studies by Berlin (2000) on political risks in oil & gas industry reveal that political risk management in the energy industry plays an increasingly important role since the world's oil and gas production pattern is directly related to the geopolitical location of reserves. Major oil reserves are located in the regions of the world characterized by an unstable political environment due to ***'accidents of geology'*** (Noreg, 2002).

Berlin (2000) further broadens the definition of political risk to include ***creeping expropriation*** which stems from changes in legislation that affect the industry such as taxes, labor, environmental regulations and other economic measures. Both third world

and even the US itself may be considered to present somewhat of a political risk to the oil & gas industry Wagner (2000).

According to Wagner (2000), Firm-specific political risks are risks directed at a particular company. By contrast, country-specific political risks are not directed at a firm, but are countrywide. Government risks are those that arise from the actions of a governmental authority, whether that authority is used legally or not. Instability risks, on the other hand, arise from political power struggles. The distinctions between different categories of political risks are summarized in the matrix next page.

	Government Risks	Instability Risks
Firm Specific Risks	• *Discriminatory regulations* • *"Creeping" expropriation* • *Breach of contract*	• *Sabotage* • *Kidnappings* • *Firm-specific boycotts*
Country Level Risks	• *Mass nationalizations* • *Regulatory changes* • *Currency inconvertibility*	• *Mass labor strikes* • *Urban rioting* • *Civil wars*

Wagner (2000) further adds that the degree of willingness to accept political risk varies from company to company. What one company finds acceptable, may be too risky for another company. In addition, there is usually a direct correlation between the degree of political risk that a company is prepared to accept, and the degree of geological potential of the proposed contract area. Effective political risk management requires distinguishing developments that pose true risks, a well-defined threat to corporate performance, from political events that are merely dramatic.

The Institute of Risk Management (UK), ALARM The National Forum for Risk Management in the Public Sector (UK) and The Association of Insurance and Risk Managers (UK) have recommended a model to summarise examples of key risks and shows that ***some specific risks can have both external and internal drivers*** and therefore overlap the two areas. They can be categorized further into types of risk such as strategic, financial, operational, hazard, etc.

Technical risks include aging facilities. In the US, refineries today are operating well into old age—some even beyond their original design life. Many facilities were built in the 1960s and are now over 40 years old (Carroll & Gosselin, 2004). In the GCC, refinery units are 75 years old and they are improved incrementally through various revamps and debottlenecking initiatives. Reliability studies have shown that that loss frequency increases exponentially once equipment has reached and surpassed the end of its design life. Furthermore, the technology and design in older plants is at a level far different then technology used today in new construction, leading to ***Technical risks***. In both upstream exploration and extraction and downstream production of oil products, technology plays a pivotal role. While some processes are commonly known and used throughout the industry, most are patented or proprietary and are the source of important competitive advantage. Most oil & gas companies take care to prevent ***risks due to leakage of sensitive IPR*** (intellectual property rights) by employees or third parties involved in the business processes.

Operational risks also include the workforce experience and a weak Business Continuity Plan (BCP). Based on various conference presentations, the oil, gas and petrochemical industry has increasingly lost experienced personnel from mergers, restructuring and retirement and migration to other attractive sectors like IT, banking, real estate etc. People with the institutional knowledge necessary to operate the facilities under all conditions are not being replaced, leaving personnel operating complex facilities with less experience needed to deal with a crisis. Again, this lack of experience increases the potential for loss when normal operation processes fail. These have been termed as ***HR risks*** in the broad sense (Proceedings in the MEOS Summit, Bahrain, 2007).

2.6 The Growing Influence of COSO ERM framework

Bernstein (1996) who chronicled the evolution of risk in his bestseller 'Against the Gods – The Remarkable Story of Risk', states that, *'The demand for risk management has risen along with the growing number of risks'*. While Kennedy (2001) adds that, *'The very*

character of our society is at risk' and also metaphors risk management to *'fighting an elusive enemy'*.

Paradigm shift in Risk Management

Before we could appreciate the emerging popularity of ERM, the paradigm shift that has emerged in risk management is presented below. The following paragraphs are culled out from various works by authors and reports from prominent risk consultants like Ching (2007), Niehaus et al (2004), James Lam & Associates (2006) and Professional Risk Managers' International Association (PRMIA).

ERM framework fundamentally redefines the concept of risk. ERM framework deliberately changes the way in which risks and risk domains are characterized and viewed. Within the ERM framework, risks and risk domains are viewed as a larger space, eliminating the artificial barriers that have traditionally been used to identify and constrain risks. ERM is a structured analytical process that focuses on identifying and estimating the financial impact and volatility of a defined *'portfolio of risks'*. ERM seeks to provide a common metric and discussion platform for top management decision making.

Ward (2006) states that, 'a major advancement on the more traditional approach, where the ***business silos*** and support functions manage risk separately and discretely, where there is no ***consistent or complete view of risk***, and where internal audit emphasizes the ***compliance aspect*** of risk management.' ERM has taken an evolutionary path and hence it is a paradigm shift and not a replacement of risk management. With any paradigm shift, the strengths of the older perspective must be accommodated and improved in the new framework (Kuhn, 1962).

The silo based approach to risk management or traditional or older risk paradigm asserts the following:

- The older risk paradigm conveyed a static definition of risk, where the probability of loss was the only expected financial outcome. The key to risk management was to mitigate the probability of losses through aggressive loss control and where ever loss could not be controlled, insurance was the recourse. A core assumption was that an organization's future performance was a function of its historic performance and this relationship was assumed to be linear.

- The older risk management paradigm assumed that risks were best handled within their functional silos. The approach further contends that successful risk mitigation within the silos were additive and provided the organization with a positive cost of risk. The problem was that the definitions of risk and the metrics used were generally different. There was no common metric tied to financial or operational performance to determine if the risk management approach was producing intended results.

- Under the older risk paradigm, '*a leap of faith*' was required to believe that risks were being identified and measured correctly, and that sufficient risk treatment was being applied to prevent serious or catastrophic cash flow impairment.

- The traditional risk paradigm asserts that partial or full risk transfer into an organized market maximizes shareholder value.

According to Shaw (2005), corporate management of risks of various types has been handled in isolated silos. He reports that the problem in the silo approach is that it entirely misses two critical aspects of risk management from a corporate, or ERM, perspective: corporate risk appetite and the management of emergent risks. Shaw suggests seven steps to implementing an effective ERM program for any organization: Assemble and educate a cross-functional team representing each significant functional Area of business, identify risks and opportunities, determine risk tolerance, identify correlations among risks and opportunities, prioritize risks and opportunities, determine appropriate actions for mitigating risks or exploiting opportunities as necessary, and put

an ERM system in place to monitor and respond to events and trends on a continual basis. Shaw also suggests that it is very helpful to have a risk management consultant assisting the business in the ERM process.

The new risk paradigm builds upon the traditional model by asserting the following:

- New risk paradigm declares that *'risk is capital'*.
- The ERM framework asserts that like other elements of the classical economic production function (capital, technology, raw inputs), risk represents a source of capital, particularly if the corporation is capable of identifying and managing its risks better than its industry grouping or immediate competitors.
- This perspective also assumes that risks do not exist in silos, but can be observed across various domains. In this framework, risks are better managed in portfolios.
- This perspective also assumes as a result of the non silo approach, a new type of organizational structure, commonly called the Enterprise Risk Management, Chief Risk Office, or Enterprise Risk Committee, are now gaining importance.

- An important ERM element is that it encourages multidisciplinary interaction within the organization.

According to COSO, ERM framework addresses the scenarios wherein the organization is replete with risks thereby strengthening the paradigm shift. It has been designed to enhance capability to:

- **Align risk appetite and strategy**
  Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.

- **Link growth, risk and return**
  Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify

and assess risks, and establish acceptable levels of risk relative to growth and return objectives.

- **Enhance risk response decisions**
  ERM provides the rigor to identify and select among alternative risk responses like risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.

- **Minimize operational losses**
  Entities have enhanced capability to identify potential events, asses risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.

- **Identify and manage cross-enterprise risks**
  Every entity faces a myriad of risks affecting different parts of the organization. Management needs to not only manage individual risk, but also understand interrelated impacts.

- **Provide integrated responses to multiple risks**
  Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.

- **Seize opportunities**
  Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.

- **Rationalize capital**
  More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

Towards greater appreciation of ERM system

ERM is now gaining importance in various industries across the world as mentioned earlier. The COSO ERM is becoming a de facto worldwide standard for assessing internal controls and risk management thereof, one could expect that COSO ERM will be going forward (Moeller, 2007). Its multidimensional format, which covers all aspects of risk management activity, seems superior to any of the enterprise risk frameworks proposed till date.

As many professionals become familiar with the COSO ERM, there is a growing appreciation of this framework and some recognition, first in the US and now worldwide (Moeller, 2007). There is a growing recognition of the need for a worldwide risk management standard and ERM is becoming a major influencing factor. Familiarity with American standards and guidelines coupled with US being the dominant world power in economics and business, other countries like in the Middle East use COSO ERM framework.

A bevy of new reports and studies that have been issued since 2005 that suggest ERM is starting to gain acceptance (Moody, 2005). Unlike the COSO Internal Control Framework, COSO ERM Framework is becoming a much more an important tool and has a much faster adoption by companies. Some of the reasons as discussed by are:

- Recently, debt rating agencies such as S&P, Moody's, and Fitch have announced their examination of ERM practices of institutions as part of their credit-rating assessment processes (Beasley *et al*, 2007).

- COSO internal controls were really launched before the pervasive use of Internet Technology and applications. Beyond COS itself, professional organizations like IIA and its consultants like Protiviti have published excellent guidance materials on ERM (Moeller, 2007).

- Because of the internal controls framework model, COSO ERM is easier to understand and use (Moeller, 2007).

- Managing risk has also become increasingly complex with the implementation of Sarbanes Oxley Act (SOX) by various companies which also include oil companies world-wide (Beasley et al, 2004).

- The phenomenon of risk has become a much more accepted concept especially after the 9/11 incident in the US, Madrid and London attacks. This has no relation to ERM, but has triggered management thinking about risks and risk management (Moeller, 2007; The Conference Board, 2005; Mercer, 2005).

- Increased accountability at the senior management and board levels has all combined to significantly change the landscape of risk management today. (Deloitte report, 2005; Mercer, 2005).

- COSO ERM concerns and impacts people beyond the executive offices and Boardroom. ERM is more pervasive to other functions like marketing, projects, engineering, IT, procurement, HR, production, operations etc in an organization. It is not just the concern of the finance function alone (Moeller, 2007; Tallinghast - Towers Perrin, 2001).

- Unprecedented complexities of the regulatory environment are pressing firms for better risk reporting and more integrated and comprehensive risk management. The complexity is further exacerbated by the increasing need for knowledge of local laws and customs, evolution of trading markets, extensive use of information technologies and higher accountability standards for boards of directors and senior executives (Deloitte report, 2005).

The reason why an ERM system in general should be implemented is discussed below. Following that the value addition through the COSO ERM is discussed to set the tone for the subsequent sections in this study.

The Conference Board's recent study, 'From Risk Management to Risk Strategy', points out, 'Recent interviews indicate that ERM is gaining currency as a comprehensive approach for evaluating activities and assessing the multitude of risks associated with conducting business' (Moody, 2005). According to Moeller (2007), ERM provides an organization with the processes it needs to become more anticipatory and effective at evaluating, embracing, and managing the uncertainties it faces as it creates sustainable value for stakeholders. It helps an organization manage its risks to protect and enhance enterprise value in three ways.

1) It helps establish competitive advantage.
2) It optimizes the cost of managing risk.
3) It helps management improve business performance.

COSO ERM contributes to an organization through the elevation of risk management to a strategic level by broadening the application and focus of the risk management process to ALL sources of value, not just physical and financial ones. Many are looking to COSO ERM for guidance due to following reasons as noted by AOL Risk Consulting:

- One of the first frameworks on the market.
- Provides transparency.
- Develops framework for meeting financial disclosure requirements.
- Promotes better decision-making, enhances capital allocation.
- Supports regulatory and compliance initiatives.
- Creates a formal link between operational, financial and strategic decision-making within the organization.

More recently, in early 2008, Standard & Poor's (S&P) communicated that the agency is enhancing its rating process globally for non-financial companies to include a review of their ERM processes and procedures. S&P will begin to hold ERM discussions with rated

companies in the third quarter 2008 and will begin to include commentary in S&P reports in the fourth quarter 2008. Even though these discussions will begin in 2008, scoring of companies' ERM capabilities will not take place until 2009, which will allow for a sufficient number of reviews to support reliable benchmarking and published evaluation criteria (AON Risk Consulting).

One of the goals of this assessment process is to evaluate the extent to which corporations approach risk management from an integrated, company-wide perspective. S&P is particularly interested in two areas:

- Strategic Risk Management
- Risk Culture and Governance

The focus is therefore on how management addresses the risks to their strategic plans and embeds a culture of risk awareness across the organization. Processes that help the understanding, managing, and communicating information about risks arising throughout the enterprise will be scrutinized. This will ultimately impact management ability to interpret and make qualitative judgments in response to various risk metrics. This ERM assessment process will not replace any current evaluation criteria, but rather enhance the appraisal of management's ability to manage key risks. Therefore, top management of S&P rated corporations need to demonstrate an ability to incorporate risk information as a part of their strategic decision making process in order to score well on the S&P ERM assessment (AON Risk Consulting). The ultimate of goal of ERM is to help management in achieving Corporate Objectives (Dickinson, 2001); ERM is also an emerging and maturing as a result of initiatives from at least two perspectives: 'A finance-driven shareholder value Model' & 'Compliance-driven risk governance Model' (Power, 2004; Dickinson, 2001; Dickinson, 2005; Lam, 2003). A KPMG survey in 2008 indicates that more than 90 % of survey respondents have ERM programs in place and see it as an opportunity to improve decision-making and increase shareholder value. They also agree that ERM is also clearly a *'Boardroom priority'*. Furthermore, within the insurance sector, Tuten (2005), states that 'compliance' and 'governance' programs drive the application of ERM, the resulting convergence is increasing the demand for ERM to the expectation of an $80 billion market over the next five years (until 2010). He also adds

that unfortunately, executives focus on ERM's expenses as necessary for compliance and miss its potential return on investment.

2.7 The present state of ERM in the Risk Continuum

Various authors and management consultants present models for maturity of risk management systems. Management Consultants have brought a breadth of knowledge and practical experience around ERM. A practical and rational method according to KPMG on risk continuum can be defined through three levels of maturity i.e., 'Basic', 'Mature' and 'Advanced' positions in their sophistication of risk management, as described below.

- **Basic** : The generally meets basic internal and external stakeholder risk management expectations and organizational requirements.
- **Mature** : Activities and techniques are employed for enhanced stakeholder confidence that risks are being managed effectively.
- **Advanced** : Risk management is seen as a strategic tool to help enhance performance and is a core value of the company.

Walker & Shenkir (2007) discuss about the ERM Maturity Models in one of the Statements of Management Accounting. They state that on implementation of ERM; the next aspect is to know about the progress made in ERM for any management. This has led to the development of a number of ERM maturity models. They state that in one organization has categorized ERM development into three phases:

(1) *Phase 1: Building a foundation* - involves building executive support, building the core model, aligning expectations, and developing segment-level risk management commitments.

(2) *Phase 2: Segment level ERM* - covers executing a consistent risk framework, engagement in specific areas and by segment-level personnel, and demonstrating the tangible value of a disciplined process.

(3) *Phase 3: Enterprise-level ERM* - includes connecting segment risks, enhancing coordination and integration, and deepening risk management focus.

Furthermore, they also add that, this approach is scalable to organizations of any size. Maturity models do more than inform a company of its progress in ERM. They can influence a company's rating from rating agencies, too. S&P now applies an ERM maturity model to certain companies and industries, such as the insurance and banking industries as well as some energy companies. Consequently, ERM implementation could eventually impact a company's cost of capital and capital adequacy. S&P evaluates an insurer's ERM practices by considering the risk management culture, risk controls, emerging risk management, risk and capital models, and strategic risk management. These lead to an ERM score of weak, adequate, strong, or excellent.

Before we could appreciate the current state of ERM, it is important to understand the limitations and benefits of this system. According to various reports from management consultants and professional bodies the position of the ERM seems to reside in debatable location along the risk continuum. Most of them cite that the state of ERM is different in every business sector ranging from a mature stage in Banking and Actuarial sectors to pilot or basic stages in Energy, Oil & Gas and Mining sectors.

The benefits and limitations of ERM have been already cited by the COSO ERM framework as one it's many objectives. The framework has been designed to serve a common basis for the following segments at interest:

- Board of Directors
- Managements
- Regulators, Internal Auditors
- Risk Personnel
- Professional Bodies/Organizations
- Academics/ Educators

The benefits have been elucidated in the earlier sections (see section XX) while the limitations are presented below.

While ERM helps management achieve an entity's objective, it does not ensure or guarantee an entity's success, no matter how well the ERM system is designed and operated. The achievement of objectives is affected by limitations inherent in all management processes like:

- Shifts in government policy, competitors' actions or economic condition can be beyond management's control.
- Human decision making can be faulty, and breakdowns can occur because of such human failures as simple error or mistake.
- ERM cannot change an inherently poor manager into a good one.
- Additionally, controls can be circumvented by the collusion of two or more people at any level.
- Management has the ability to override the ERM process, including risk responses and controls.

The design of ERM must reflect reality of resource constraints, and the risk management benefits must be considered relative to their costs. Therefore, while ERM can help management achieve its objectives, it is not a panacea. Many management researchers have tested and acknowledged that the above benefits and limitation of the ERM system is ubiquitous to most organizations trying to embrace and sustain the COSO ERM system.

In light of the benefits and limitation of the ERM system, the present state and the plausible future state of ERM is discussed in Lam's Ten Predictions for Risk Management (2003) predicting the following:

1. **ERM will become the industry standard for risk management.**
   Leaders of ERM will continue to produce more consistent business results over various economic cycles and better than their competitors. Their successes will gain attention and other companies will follow. Mature ERM companies will continue to highlight the pitfalls of the traditional 'silo' approach to risk management.

2. **A Chief Risk Officer (CRO) will become prevalent in risk-intensive businesses.**

The rise of the CRO goes hand-in-hand with the trend towards enterprise risk management. Companies without a CRO are faced with three perplexing questions:

(A) Are we comfortable with diffused risk responsibilities, and if not, who is the de facto CRO. Is it the CEO or CFO?

(B) Are their necessarily part-time efforts sufficient in managing risk in an increasingly volatile business environment?

(C) Will the company be able to attract and retain high caliber risk professionals if a CRO career track is not available to them?

For an increasing number of companies, the logical resolution of these questions will be the appointment of a CRO and the dedication of resources to implement an ERM program.

3. **Audit committees will evolve into risk committees.**

As Boards of Directors recognize that they have responsibilities to ensure that appropriate risk management resources are in place, they will replace or supplement their audit committees with risk committees. A number of leading institutions have already established risk committees of the Board. The Board's responsibilities for risk management have been clearly established in the SOX, as well as corporate governance initiatives such as the Dey, Turnbull, and Treadway Commission Reports. The result of these and other similar initiatives is that board directors have begun to realize that their responsibilities go beyond traditional audit activities, and that they need to ensure resources and controls are in place for all types of risk. Regardless of its name, the audit committees of the future will have enterprise-wide risk management scope.

4. **Economic capital will be in and VaR will be out.**

Managers and external stakeholders will demand a standardized unit of risk measurement, or common currency, for all types of risk. This way, they can spot

trends in a company's risk profile, as well as compare the risk/return performance of one company against others. To date, VaR has gained wide acceptance as a standardized measure for market risk. However, VaR has three major flaws.

(A) It does not capture "tail risks" due to highly infrequent, but potentially devastating, events.

(B) Its inability to capture tail risks makes VaR a poor measure for credit and operational risks (or even market risk positions with significant optionality).

(C) VaR measures the risk, not the return, of any risk position.

Yet financial models that have passed the test of time, such as CAPM or the Black-Scholes option pricing model, evaluate both risk and return. The concept of economic capital is intuitively appealing because one of the main reasons companies hold capital is to absorb potential losses from all types of risk. Risk-adjusted return on capital extends the concept and measures business profitability on a risk-adjusted basis. The Basel Committee has already adopted economic capital as the framework for international regulatory capital requirements in the banking industry. Other industries will follow and adopt it as a common currency for risk.

5. **Risk transfer will be executed at the enterprise level.**

The integration of risk transfer activities has already happened as far as hedging and insurance strategies are concerned. For example, companies that hedge with derivatives realize they can save on hedging costs if they execute portfolio hedges rather than individual securities hedges. Companies that bundle their insurance coverage through multi-risk multi-year policies are also realizing significant savings on insurance premiums. Alternative Risk Transfer (ART) goes one step further in combining capital markets and insurance techniques. The rise of ERM and ART products will mean that risk transfer strategies are increasingly formulated and executed at the enterprise level. In the past, companies made risk transfer decisions to control specific risks within a defined range, without being particularly thoughtful about the cost of risk transfer unless it was prohibitively

high. In the future, companies will make risk transfer decisions based on an explicit comparison between the cost of risk retention versus the cost of risk transfer and execute only those transactions that increase shareholder value.

6. **Advanced technology will have a profound impact on risk management.**
   The Internet (and Intranet) will have a significant impact on risk management and how information, analytics and risk transfer products are distributed. Beyond the Internet, the increase in computing speed and decline in data storage costs will provide much more powerful risk management systems.

7. **A measurement standard will emerge for operational risk.**
   There is considerable debate not only about the quantification of operational risk, but also how to best define it.

8. **Mark-to-market accounting will be the basis of financial reporting.**
   The use of mark-to-market accounting is widely accepted in the market risk field, and is gaining acceptance in credit risk management. Over time, the risk management profession has recognized the importance of mark-to-market accounting versus accrual accounting in reporting the financial condition of a company.

9. **Risk education will be a part of corporate training and college finance programs.**
   Given the rising corporate demand for skilled risk professionals, professional organizations and colleges will continue to integrate risk management into their course offerings.

10. **The salary gap among risk professionals will continue to widen.**
    The trend towards ERM and the appointment of CROs has created an exciting career path, and attractive compensation opportunities, for risk professionals. However, this new career opportunity will only be available to risk professionals

that continue to develop new skills and gain new experiences, while the others will be left behind.

While comparing Lam's predictions and the present state as of 2008, when this study is made, there seems to be a realistic correlation with his predictions and the Boardroom thinking. The Conference Board (Canada), a business research organization, and consulting firm Mercer Oliver Wyman, based on a survey of 271 risk management executives; state that companies are seeing benefits from ERM even in the early stages of implementation. Among businesses with limited risk assessment programs, 58 % said that ERM has helped them improve decision-making. That proportion climbs to 86 % among companies with full-fledged ERM programs. Therefore, we can surmise that ERM is gaining ground, but slowly. Most organizations are still in the process of building the foundation for their ERM infrastructure (Cummings, 2005).

This study will try to better understand the management inertia to achieve success through an effective ERM system, especially in GCC Oil industry.

2.8 Testimonials and User Feedback on COSO ERM Framework

'The Good, the Bad and the Ugly' on the COSO ERM framework is now reviewed to understand its strengths, weaknesses, threats and opportunities from entities reporting *early wins* and *fence sitters*, including commentaries and opinions from representatives of the professional bodies representing COSO and other specialist risk practitioners. There are controversies surrounding the framework and according to Lam (2006), ***"any framework has limitations."*** He argues that in most cases, an entity is better served by integrating the principles from COSO ERM and other frameworks and implementing a customized approach.

Stinging indictments on COSO ERM

In his risk commentaries, Kloman (2006) has come out and stated that, "The beast [COSO] has at last produced its expected offspring. Given a gestation period of over

three years, we might logically expect something that could go forth and be useful, but, alas, this creature is preceded by smaller, clearer-eyed, and more nimble adversaries [lesser-known ERM models], leaving it to lumber away from its five parents (a biological marvel!) and gather dust when it finally comes to earth." "I'm afraid its ***monstrous size*** [230 pages] and ***tedious prose***...will condemn it to the dust shelf,"....."But because of the sheer volume of interest today in risk management.....***COSO's version will receive broad distribution***. It doesn't deserve it."

Quinn (2006) states that, some criticize that the framework is too simplistic and principles based and includes little implementation guidance. Among them, the American Academy of Actuaries (AAA), feel strongly that COSO ignored their comments. The Academy's concerns voiced out are: The model focuses too much on 'adverse outcomes' rather than the ***potential upsides of risks*** and ***pays too little attention to 'external risks'*** that companies face. Some Deloitte and PwC's reports concede that the extraordinarily ***poor timing*** of its introduction was when companies had wrapped up their obligations under Section 404 of SOX. This meant yet ***another extra layer of compliance*** work which wasn't received well in many organizations. Most COSO sponsoring organizations had ***failed to work*** actively with members on the ***implementation aspects*** on the ground. It is reported that several critics think that COSO ERM is tougher even than the internal controls framework to implement; and it is also more ***challenging to take from the theoretical to the practical***, and there's a greater diversity of views of how you do it; requiring even more study on functional and technical involvement than the internal controls framework.

Kloman (2006) also states that, "COSO falls into the fatal fallacy of trying to tell us *how* to do it rather than *why*." A similar viewpoint is shared by S&P's one of the ERM Directors Samanta (2006), "What a large number of issuers are grappling with is exactly how they should go about putting together an ERM program. That's where there's a need for guidance. COSO ERM's great in terms of documenting what an ERM program should look like, but the hole is: How do I implement it? It's needed particularly by the industrials and energy and utility companies." Walker (2006) also opines that framework

counterparts from other countries seem more focused than COSO ERM and doesn't drag out to get to the point.

Quinn (2006) reports that, many companies say COSO has failed to clearly define what the Securities & Exchange Commission SEC has and hasn't said about COSO ERM. Some critics also say that SEC has failed to clearly explain the differences between COSO '92 and COSO ERM and what it requires as well. Interestingly, it is also reported that the agency has no point person on COSO per se or COSO ERM or risk management in general.

In defense of COSO ERM

From a corporate point of view, Minter (2006), ex-President of IMA, states that COSO's ***sponsoring organizations should be beating the drum*** to get the to get information about COSO ERM out to companies. Many companies think they can ignore these ongoing debates about ERM in general and COSO ERM in particular precisely because there's no regulatory or legal requirement to heed. Ignoring them, however, may be at their own risk. For one thing, ratings agencies, analysts, and exchanges across the globe are now focusing on risk management in their ratings decisions and are aware that ***COSO ERM is rapidly becoming the preferred model.***

Rittenberg (2006), Chairman of COSO, admitted states that, "The reluctance within US corporations to adopt COSO ERM is true" while Lam (2006) has stated that in his opinion, "it's growing overseas". Leech (2006), a great proponent of SOX gives a neutral opinion saying that, "Unfortunately, ***basing COSO ERM on COSO '92 was a mistake***". He states that a lot of progress has been made since then around the world that is worth recognizing, which COSO ERM should have embraced without taking a cue from COSO '92 coming from a pure internal controls perspective. Rittenberg (2006) also argues that although there are controversies surrounding this framework, there is no reason to modify it. He argues that, it is a ***powerful framework across multiple disciplines and there is no need to reinvent it.*** He urges that a lot of organizations can take individual components

such as identifying risk and talk about ways that that can be improved for them individually. The framework does not go to that level of specificity and organizations can implement best practices over time and still be consistent with the framework.

While Raymond (2006). states that, this framework is ***an accountant's approach to risk management*** and it is not as broad based as you need to have, but however accepts it a worthwhile tool which is very amenable and good for purposes of internal audit. Malmquist (2006), states that there needs to be ***a sell-in to the 'C-suite' offices*** as business community has not fully accepted the need for ERM and by extension COSO ERM because it has a difficult time determining or deciding what is different about ERM from what it does daily in managing operations. While SOX has brought ERM into the spotlight a little bit, but the business community hasn't fully put its arms around ERM yet. While Quinn (2006) reports that a recent Conference Board of Canada survey has found that companies in Canada use a framework and the ***most commonly used framework is COSO ERM***. DeLoach (2003) states that ERM framework has been built on the foundation laid by SOX.

Mc Namee (2004) has explained why ERM is important. According to Mc Namee, ERM is required because of the following reasons: "A means to stimulate imagination combined with a deep understanding of the business." "A method of accumulating and sharing what is accumulated .....including a common language." "...overly complex methods are likely never to be fully implemented, or, if they are, to generate a lot of resentment, non-compliance and workarounds." "...***the minutia will be well-managed at great cost while ignoring the big picture***, especially the future types of risks."

COSO proponents say that ***implementing COSO ERM makes sense*** as a follow-up to their SOX 404 control efforts and is a way to extend those efforts from the financial arena to the entire organization. Leech (2006) adds that companies may find themselves stuck with COSO ERM by default, simply because it's better known than the other existing models and ***made in the USA*** branding regardless of whether it's the model that best suits

their needs. Furthermore, COSO ERM has also fiercely fought defended their product by clearly explaining that there is no amendments and revisions required to be made.

Some proponents feel that COSO has done a wonderful job in issuing ***ERM guidance that is relevant, applicable, and useful.*** Professional bodies and the Big 4 have provided a variety of reference documents and procedures that enable executives to organize their SOX 404 programs effectively and ERM perspectives have enabled businesses to reap benefits. They believe that COSO has been on the right path for the past decade precisely because it has focused first on financial controls. And now it is focusing on risk management which is the next wave in terms of what needs to be tackled (Quinn, 2006).

Everson (2006) presents an interesting argument in favour of the framework. While drawing the attention to think about the alternatives to this framework, he approaches the problem with an enquiry; if it is best for companies and the capital markets to have one framework for capital markets and another one for risk management? It would not be helpful and productive with the interrelationships between risks, there will be too much interdependence to create separate frameworks. One would create more problems than resolving it through a new framework. Beasley (2006) an academician states that, "The beauty of the COSO framework is that it has been ***put together through due process***. So if in the future a company has to say publicly that it has effected an ERM framework, it will be able to ***reference one that is publicly accepted***. I give COSO as an organization an A+ on this." He also adds that, "It's way too early to say whether COSO ERM is widely embraced because people aren't at the point where they have to assert publicly what they're doing against it. Meanwhile, I think it's important for COSO's five sponsoring organizations to help companies consider an ERM framework." This comment gels with Minter's (2006) opinion on the COSO members.

Studies by Ballou & Heitger (2005) conclude that "The goal of the framework is to enable organizations to ***standardize enterprise risk management*** (ERM) so that organizations can more easily benchmark, establish best practices, and have ***more meaningful dialogue*** about the critically important issue of risk management. One

concern regarding the COSO ERM framework is that its ***overreaching nature can appear overwhelming for some organizations***, particularly those that are small in size or have not previously established an ERM culture." Adams & Campbell (2005) report that many CFOs are looking at ERM as a way to leverage their significant investment in compliance and convert it into a shareholder value strategy like cost containment or revenue enhancement strategies.

Threat of new regulation

Quinn (2006) states that there is a huge fear in the corporate community that companies will be required either by legislators or regulators to attest that they have an effective program in place. Malmquist (2006), states that many businesses are reluctant to incur additional costs unless there are obvious benefits. Otherwise, it just waits for something to be legislated. Studies on alignment of corporate governance and ERM by Sobel & Reding (2004) mention that a practical, ***how-to guidance*** for executives, managers, and auditors who are involved in corporate governance on a day-to-day basis in ERM settings ***is sparse.***

Emerging opportunities

Institute of Management Accountants has recently published a new internal controls assessment model to supplement the COSO ERM framework, by addressing the weaknesses in the framework; thereby improving its effectiveness. Converting the looming threat mentioned earlier into an opportunity by introducing a new risk standard with superior standing than the COSO ERM framework of 2004.

According to the SEC, suitable frameworks must be "free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting." Therefore some companies are of

the opinion that ***the final rules do not mandate use of a particular framework*** in recognition of the fact that other evaluation standards exist outside the US and that frameworks ***other than COSO may be developed*** within the US in the future that satisfy the intent of the statute without diminishing the benefit to investors" (Quinn, 2006).

Following cue from other professional bodies, like the Financial Accounting Standards Board (FASB) and the International Accounting Standards Board (IASB), which had issued their pronouncements and then let the organizations decide as to how to implement them and make it workable, and later provide guidance for their support services at a cost, perhaps COSO may also be ***going akin to Accounting Standards setters*** in the near future (Quinn, 2006). Furthermore, there is also a possibility of all the professional bodies dealing with risk (Actuarial societies, PRMIA etc) to converge and collaborate thereby promoting a multidisciplinary platform and not an accountant's area of interest.

The 2005 Financial Executive Report on Risk Management by Oversight Systems Inc. reports that despite the fact that ERM is one of the hot strategic business tools that companies are employing, ***many firms still have a long way to go toward proper execution***. In most of the businesses, the critical elements of risk management are not in place. Most of the financial executives in the Oversight Systems survey responded that they were best prepared to assess financial reporting risk and that they were planning to leverage what they found during SOX compliance into an ERM program.

2.9 Integrating ERM into a changing business environment

When ERM is seen as sound business management rather than the management fad of the month, it becomes an integral part of the organization's DNA. Walker et al (2006) have stated that some of the opportunities for integrating ERM in ongoing management activities include:

- Strategic planning
- Balanced Scorecard
- Budgeting

- Total Quality Management and Six Sigma
- Business continuity
- Corporate governance
- Risk disclosures

Strategic Planning

The COSO definition of ERM states that ERM is part of strategy setting. ERM and strategy setting should be viewed as complementing each other and not as independent activities. If strategy is formulated without identifying the risks embedded in the strategy and assessing and managing those risks, the strategy is incomplete and at risk of failure. Similarly, if ERM does not begin with holistically identifying risks related to the company's strategy, the effort will be incomplete by failing to identify some very important risks (Walker et al, 2006).

An article in the Economist Intelligence (2001) states that a study by Mercer Management Consulting analyzed the value collapses in the Fortune 1000 during 1993-1998. The analysis found that 10% of the Fortune 1000 lost 25% of shareholder value within a one-month period. Mercer traced the collapses back to their root causes and found that 58% of the losses were triggered by strategic risk, 31% by operational risk, and 6% by financial risk. Hazard risk did not cause any of the decrease in shareholder value.

Kocourek et al (2004) state that Booz Allen Hamilton analyzed 1200 firms during 1999-2003 with market capitalizations greater than $1 billion. The poorest performers were identified as companies that trailed the lowest-performing index for that period, which was the S&P 500. The primary events triggering the loss of shareholder value were strategic and operational failures. Of the 360 worst performers in the study, 87% of value destruction suffered by these companies related to strategic and operational mismanagement.

According to Walker et al (2006), when formulating the company's strategy, top management analyzes its strategic alternatives and identifies events that could threaten their achievement. As the risks embedded in each strategic alternative are identified and placed on a risk map, the alternative can be evaluated against the organization's capabilities and how it aligns with the risk appetite. Strategy formulation is enhanced by ERM because risks are identified and the strategic alternatives are assessed given the company's risk appetite. In turn, without a well articulated strategy, the foundation for implementing ERM is insufficient. Viewing the two together forms the basis for a strategy-risk-focused organization.

Balanced Scorecard (BSC)

Kaplan and Norton (2001) devised today's ubiquitous tool for communicating and cascading the company's strategy throughout the organization through their BSC management system. The conventional BSC captures the company's strategy in four key perspectives i.e., Customer; Internal; Innovation and learning; and Financial. Nagumo and Barnaby (2006); Nagumo (2005) have recently validated their studies in the Bank of Tokyo and Mitsubishi that by combining the BSC with ERM, entities can enhance performance management. In the BSC, objectives are identified for each of the perspectives, and, as noted previously, ERM begins with an understanding of objectives. For each BSC perspective, metrics (KPIs) are selected and stretch targets are set. ERM adds value to the BSC through the identification of events (risks) that could stand in the way of achieving the targets in each of the four perspectives. By monitoring the KPIs, management can assess how effectively their risk mitigation efforts are working. In effect, the KPIs for each perspective also serve as key risk indicators (KRIs), although they are not initially selected for that purpose. Walker et al, (2006), explains that the conventional BSC can be integrated with ERM to manage and monitor risk related to the strategic objectives. Using a risk scorecard for the key risks identified in each of the BSC perspectives is a way to assign responsibility for managing the risk.

Budgeting

A company's budget reflects the current-year financial commitment to achieve the organization's long-term strategy. According to Walker et al, (2006), the annual budget can be integrated with ERM to provide insights on what the strategic business unit's leadership sees as the threats to meeting its financial plan. A risk map presented with the unit's budget provides information to senior management on what the major threats are to meeting the financial plan for the year. The risk map gives senior management a point of departure in the budget review process without having to waste time uncovering the implicit budget risks. Operating units should know their risks if they are to have any chance of accomplishing the plan. An additional benefit of including a risk map on the budget risks is that, as the various budgets and risk maps are reviewed by senior management, they can compare the risks they have identified in the strategic plan with those identified by the operating units. Furthermore, senior management can ask questions about the expenses in the budget that relate to risk mitigation decisions for the high impact/high likelihood risks.

Total Quality Management and Six Sigma

Walker et al, (2006) recommends that quality initiatives focus on improving the efficiency and effectiveness of detailed processes. ERM requires clarity of objectives at all levels of the enterprise, and the objectives of specific processes can be addressed by utilizing quality tools and methodologies. When an organization has implemented a quality initiative, information is available on detailed processes. In turn, this information can be evaluated within the larger context of the enterprise to identify risks in an ERM implementation. Also, quality initiatives can provide information on planning the mitigation action for a process risk.

Business continuity

Barton et al (2002) state that regardless of how robust the effort of risk identification is, some unknown risks will remain unknown at the end of the process. A company prepares for these unknown risks through its business continuity, or crisis management, plan—an

essential element of the ERM process. They also touch upon reputation risk as a company must be prepared to recognize a crisis and respond swiftly to contain it before damage is done to its reputation and brands.

Corporate Governance

Barton et al (2001), Burns (2003), Emen (2004) and many other authors acknowledge that ERM ties in closely with corporate governance because it:

- Improves information flows between the company and the board regarding risks.
- Enhances discussions of strategy and the related risks between executives and the board.
- Monitors key risks by accountants and management with reports to the board.
- Identifies acceptable levels of risks to be taken and assumed.
- Focuses management on the risks identified.
- Improves disclosures to stakeholders about risks taken and risks yet to be managed.
- Reassures the board that management no longer manages risk in silos.
- Knows which of the organization's objectives is at greatest risk.

The flow of risk information to the board is critical in improving corporate governance. By presenting risk maps to its audit committee to keep the committee members fully informed, management communicates to the audit committee its action plans for the risks and how those risks are monitored. Furthermore, it informs the audit committee on how the risk assessment and metrics used to monitor the risk relate to shareholder value measurements.

Risk Disclosures and other Voluntary Disclosures

Emen (2004) notes that companies are disclosing more information about the risks they face. In some instances, this risk information is the result of new regulatory requirements. In others, it is a management decision.

Even if the above disclosures are made by companies, this does not mean that a company actively and continuously manages its risks as part of its strategic and operational planning processes. Boards, shareholders, and other stakeholders should want to know more about a company's ERM process. Some companies publicly disclose that they have an ERM process. Other companies disclose that they have a risk committee, Chief Risk Officer (CRO), or risk infrastructure. Still others disclose software they are using for ERM.

Similarities in COSO ERM and SOX sections

COSO ERM framework and SOX are two separate enterprise initiatives but with close relationships. There are some broad differences between the two and common threads and requirements.

- SOX primarily focuses on accurate financial reporting and related corporate governance issues.
- COSO ERM takes a broader view of things and covers all risks surrounding the enterprise.

Risk Management function would argue that COSO ERM is even more important than SOX, as it covers such a wide range of potential enterprise risks. Similarly, Corporate Finance function who could do prison time due to some fouled-up financial reporting may view that SOX violation is more significant than probabilistic estimates of enterprise risks.

COSO ERM often follows the same internal control assessment paths and has similar implications as SOX. ERM function of an enterprise has a responsibility to review risks at all levels and communicate those risks to the appropriate parties. The internal control gaps derived from SOX Section 404 also represent those type of risks identified through ERM program.

According to Hirth (2005), SOX is almost a point-by-point response to specific offenses and issues like: poor disclosure, self-dealing, and deceit; abuse of employee loans and spending; cooking the books at the top; outright fraud and bid-rigging; and much, much more. Linking them all is corporate governance, or rather, lack of corporate governance. As discussions of corporate governance have evolved, so has the concept of risk – specifically, ERM.

In many cases, it was a lack of holistic, consistent, enterprise-wide risk identification, assessment, prioritization and monitoring that created a lackluster corporate governance environment and allowed corporate governance failure to occur.

The COSO ERM framework incorporates a handful of strongly linked concepts. Each entity exists to provide value for its stakeholders. At the same time, each entity also faces uncertainty. That leaves The Board of Directors and the Management with a tough task to decide what level of uncertainty is acceptable, recognizing that uncertainty provides potential to add value as well as risk.

Similar studies have been done on the above themes like ***'Going Beyond ERM'***. McWhorter, Matherly, & Frizzell (2006) suggest a ***strategic performance measurement system*** (SPMS) to improve organizational performance, employee efficacy, and enhance the ERM system. According to these researchers, SPMS and ERM have several similar characteristics. Both encourage a holistic view of the organization. Also, when using SPMS and ERM, it is important to establish a link to organizational strategy: SPMS links with the organizational strategy through performance measures, and ERM links with the organizational strategy through risk management. Finally, both SPMS and ERM educate employees about strategic objectives.

Because SPMS and ERM share these characteristics, the researchers evaluated whether using SPMS strengthens risk management. In their study, 62% of SPMS users (compared to only 36% of nonusers), believe their organization's risk management system is a valued function within their organization. Additionally, 63% of SPMS users say their organizations encourage individuals to communicate urgent risks through their risk management system.

Furthermore, studies by Beasley, Al Chen, Nunez, & Wright (2006), suggest linkages between Balanced Scorecards and ERM. While balanced scorecards measure an organization's progress toward achieving strategic goals, ERM helps company leaders think through positive and negative factors that can affect the achievement of their goals. A core element of ERM is that risks and strategy are aligned and are integral to strategic planning and performance assessment. On the other hand, a generic balanced scorecard translates an organization's overall mission and strategy into specific and measurable operational and performance metrics across four perspectives: learning and growth for employees, internal business processes, customer satisfaction, and financial performance. These researchers demonstrate that ERM and balanced scorecard systems share many elements, including a focus on strategy, holistic perspective, emphasis on interrelationships, top-down emphasis, desire for consistency, and focus on accountabilities. Leveraging balanced scorecards into ERM actually strengthens the scope of management's focus on broader sets of risks. They conclude that it broadens the scope by explicitly linking risk management to strategic performance measurement.

2.10 Survey of COSO ERM applications in various industries

From a geographical perspective, Merrifield (2001), ERM is largely ***an Anglo-Saxon phenomenon***. "It's American, it's British and to a degree Australasian", and he believes that Europeans have a lot to catch up. Whereas from an industry perspective, Roberts (2004) states that, "Enterprise Risk Management, the new approach to risk management is gaining advocates in widening range of industries." She further adds that, "While the ***banking industry may have paved the way*** in the use of enterprise risk management as a means to identify and control risk across an entire organization, other industries are quickly following suit. Finding that ERM just makes good business sense, such industries as insurance, health care, consumer products and pharmaceuticals have hopped on the ERM bandwagon."

Ward (2006) states that ***Australian and New Zealand companies*** are embracing ERM, with many of those "at the big end of town" appearing to have ***some of the fundamentals of ERM well in place***. The survey also revealed that the risk-management strategies of the region's corporates remain fairly conservative and focused on the "downside" of risk, with respondents saying their risk-management strategies place far more emphasis on risk mitigation and preserving value than adding value and using risk information to gain competitive advantage. The composition of the survey being: 35% energy and utilities, 15% transportation, 12% materials, 12% media, communication and entertainment, 11% retail and consumer products, 9% property and construction, and 6% other. It was found that the materials, property and construction were stronger in their ERM maturity, followed by energy & utilities and transportation companies; and the rest were the least advanced in the risk continuum.

Many of the shortcomings identified in the survey were in the areas of risk-management culture and capability, which are fundamental to the success of any risk-management framework. She concludes that a lot more investment and progress is needed before many companies in the region can claim ERM is strongly embedded in their organizations. Notably, only about 50% of the respondents strongly agreed that they had a strong risk-management culture, and that the alignment of risk management and strategic objectives was something they did particularly well. The more significant ERM shortcomings stated were: Lack of a clearly articulated risk appetite, Low level of alignment between performance incentives and risk accountability, Limited priority given to effectively educating people on risk and limited progression in using risk information more strategically to capitalize on the 'upside' of opportunity.

Similarly, Acharya & Johnson (2006) have explored the scope and extent to which insurance companies manage risk holistically in four major European re-insurers. Bhaumik, Hexter & Tonello (2008) have assessed the Climate for Enterprise Risk Management in India. They state that, 'As Indian firms expand beyond national borders, they are increasingly exposed to a new array of strategic and operational risks, including those derived from different geopolitical and cultural contexts.' Their study looks at the

state of ERM integration in India-based corporations and examines emerging practices in this area by four leading corporations in India: Tata Motors Ltd., Tata Chemicals Ltd., Dr. Reddy's, and ICICI Bank. Among the key findings and trends now emerging in India with regard to ERM are the following:

- Much of the focus in ERM in Indian companies to date has been on the downside risk, not the opportunity side of the equation. Part of the cultural change that ERM brings is the understanding that ERM can help to identify opportunities and their associated risks and rewards.
- Three of the four India-based multinational companies examined in this report have adopted ERM in part because they have securities listed in the United States as well as in India. Board members at those companies believe that a comprehensive approach to managing risk is one way to satisfy listing requirements across geographies.
- The ***value proposition for ERM is not yet evident for most Indian companies.*** Most companies and boards that have begun ERM are doing so more as compliance exercise than a strategic one.

Marie & Rao (2007) have evaluated the current status of ERM in business organizations in Dubai and suggest some guidelines to help the businesses alleviate business risks. This article evaluates the current status of ERM in the business organizations in Dubai by specifically focusing on several key questions concerning businesses there. Through a questionnaire, they have surveyed business executives in Dubai to find answers to these questions: What types of risks are crucial for these businesses? How important is ERM for them? How do the companies identify and measure risk? What tools and processes are in existence for ERM, and are they adequate? How are various risks categorized by the businesses? What steps could be followed to improve implementation of ERM in Dubai? Their sample contained 51% Banks, 23% Non-Banking Finance Houses and 26% Miscellaneous companies mostly belonging to hospitality, manufacturing, trading sectors in Dubai.

The findings indicate the following:

a) Businesses in Dubai are currently implementing some aspects of risk management, but more needs to be done through an integrated strategic ERM process.
b) There is a need to create comprehensive awareness about ERM across all categories of businesses in Dubai.
c) In terms of risk management processes, survey respondents were dissatisfied most with their current ability to include operational risk in the determination of economic capital; model the important operational and financial risks both qualitatively and quantitatively; optimize financial and operational risk management strategies in light of the organization's risk/return requirements; and accurately model the impact of risks and strategies on key performance indicators.

The author's recommendations are the following to help businesses in Dubai make well-informed decisions:

1. The process involves differentiating the financial and operational risks.
2. Classifying and prioritizing strategic and manageable risks.
3. Modeling the risk.
4. Assessing the impact of risk on KPI.
5. Managing change through ERM leadership, communication, involvement, and measurement.

Finally, the authors state that ***their experiences with various businesses in Dubai have not been too positive***. They believe, however, that proactive steps by the businesses are urgently required as these businesses are experiencing strategic and operational problems such as decreasing margins, increasing competition from unconventional sources, demanding stakeholders, and too much capital pursuing too little business. All these risks lend themselves to ERM change as outlined in this article.

However, *a contentious issue is their opening premise of the studies* which states that, "The business climate in the United Arab Emirates in general—and Dubai in particular—is similar to that in other countries globally" is highly arguable.

- Dubai is a Sheikhdom with no superior corporate governance attributes comparable in the global business landscape and indeed even other GCC counterparts like Bahrain.
- The other drawback in this study is that it focuses on non oil & gas related entities and therefore may not wholly add much credence to the current study being taken up in this academic work.

2.11 A recent cry for ERM implementation in the oil & gas industry

One of the major transit oil pipelines owned by British Petroleum at Alaska's Prudhoe Bay spilled 1,010 cu m (267,000 gal) onto the Tundra, owing to failure in properly maintaining pipelines that led to corrosion and caused the largest-ever onshore oil spill, as acknowledged in the Encyclopedia Britannica. How could British Petroleum (BP), a company that has made *'Being Green'* a core part of its identity, even rebranding itself as *'Beyond Petroleum'*, suffer within one year both the worst oil spill in the history of the North Slope and the worst US refinery accident in more than a decade?

BP's oil pipeline leak in 2006 is believed and accepted as a cry for ERM system implementation (Minsky, 2006); while Fineberg's Investigation (2006) has also recommended embracing a risk based monitoring program. The immense failure of management is vividly illustrated by Schwartz's (2006) description of the oil spill that took place; as well as other reports echoing the following views on hind sight:

- Where were the smart pigs for 14 years? (Palast, 2006). Low-velocity transit lines that failed should have been pigged more often to clean it as well as monitor it for corrosion, cracks, sediment deposits, and other threats that might lead to a leak (Schwartz, 2006).
- 'The larger lack of consistency and lack of standardization across the North Slope.' (BP's quality-assurance specialist Bill Herasymiuk, 2002 as stated by Schwartz, 2006).
- 'Engineering myopia or bias in the weighting assigned to decision-making inputs regarding prevention and mitigation measures.' (Fineberg, 2006).

- 'In hindsight, obviously we wish we had been pigging. But the data we had told us we were doing the right thing' (Corrosion Expert, Bill Hedges, 2006, as stated by Schwartz, 2006).
- 'Until recently, BP's internal culture was characterized by intense pressure to keep costs down, and budgeting often took precedence over routine maintenance and occasionally over safety' (Schwartz, 2006).
- The management mantra was, 'Can we cut costs 10 percent?' (Anonymous worker, 2006, as stated by Schwartz, 2006).
- Management had an 'it can't happen here' mentality. Coupled with constant turnover worsening the situation, as new bosses would seek to beat the previous management's numbers (Schwartz, 2006).
- BP had a habit of hunting down and destroying the careers of those who warn of pipeline problems; they even ran surveillances and smear campaigns to shut whistleblowers (Palast, 2006).
- Oversight of risk management (Fineberg, 2006).

Minsky (2006) has analyzed the above incident and comes out with his recommendation. Whenever there is a disaster or event that causes losses, it is usually proven that someone or several employees in middle management or on the front lines had been forecasting the event years before but no action had been taken. The above story of BP's oil pipeline leak in Alaska is no different.

How can such bad decision making be made by such smart people? The answer is found in the ***over reliance on quantitative analysis***. There is a philosophy among some risk personnels that all answers can be found in the deep quantitative analysis of the numbers in databases to detect patterns. This is true for high frequency risks. However, for low frequency and high impact risks (like the BP oil leak) quantitative analysis will often lead to incorrect decision making or more analysis with no decision making at all.

- First, there is insufficient data historically to analyze and many possible outcomes can easily and incorrectly be 'fit to the data'.

- Second, with too little data, the patterns of correlation, dependency and therefore big picture ramifications can not be easily understood.

According to Minsky (2006), "***The solution is Enterprise Risk Management.***" ERM is an iterative and sequential series of steps that utilizes risk self-assessment (the process of identifying and evaluating risk with regard to their potential impact and likelihood, as well as related controls) as well as the subsequent risk management process of control evaluation, action plan definition, monitoring of risk- and implementation development. ERM starts with a holistic and qualitative approach to first identify all the possible root causes of an issue and then systematically help quantify the total risk consequence taking all the possibilities into consideration with scenario analysis and if needed quantitative analysis. Quantitative analysis is expensive and much focused in applicability. ERM is all about best practices of performing a self-assessment and scenario analysis before deciding where, when and how to invest in a deeper quantitative analysis like loss database approaches, wherever required. With ERM, management can prioritize the full costs versus the benefits to make a better decision. Apart from the harmful environmental impact, the aftermath of this incident on business was when the news hit the investors, shares of BP dropped coupled with panic reactions in the commodities markets.

Similar studies on the ***various BP debacles*** by Blanco & Regan (2006) also add that reputational risk is often managed in a reactive fashion. In order to maintain and enhance a firm's reputation with its various stakeholders in times of crises, ***it is critical to have a proactive enterprise-wide risk management program*** that includes crisis management and reputational risk. They however point out that many of the issues and the unfortunate public perception of BP North America were inherited from Amoco that BP now owns with problems.

2.12 Conclusion: *Emerging Research Gaps*

Analysis of Enterprise Risk Management has received more attention from the banking (Basel II, 2001; Leech, 2003; Hashagen, 2008) and insurance sectors (Solvency II, 2002) and is now a hot topic (Roberts, 2004; Beasley et al, 2007, Deloitte, 2008). Due to the

reported benefits of COSO ERM and its advocacy from rating agencies to SEC requirements, organizations in various other sectors have joined the ERM bandwagon (Lam, 2006, 2003) and is a Boardroom priority (KPMG Survey, 2008; Shaw, 2005; Lam 2003). While some organizations in various sectors are stimulated by corporate governance best practices (SOX, 2002; Moeller, 2007; Moeller, 2004; Turnbull, 1999; Carey, 2000) to consider establishment of an ERM system, Minsky (2006), Fineberg (2006), Palast (2006) and Blanco & Regan (2006) have vividly illustrated the need for a proactive ERM program in the oil & gas industry.

Based on the literature survey, it is evident that historically the management of risks has tended to be in silos (Shaw, 2005; Lam, 2003). There were serious over and under management of key risks because of the lack of an overall unified risk management effort. Additionally risks could go unidentified and fail to be managed. ERM is a new paradigm for managing Business Risks (Walker, Shenkir & Barton, 2002), is highly strategic in nature (Ward, 2006) and is an array of components (Psica, 2008), put together through due process (Beasley, 2006) within an organization that work together to manage risk over time efficiently and effectively (Moeller, 2007) and is purposefully broad in its definition (COSO ERM, 2004; Moeller, 2007; Kloman, 2005; Lam, 2003; Rittenberg, 2007).

COSO ERM which is rapidly becoming a preferred model (Minter, 2006; Rittenberg, 2006), goes beyond internal controls to provide a system to address organizational risks in a comprehensive fashion, as opposed to dealing with individual types of risks. The overall goal is to provide reasonable assurance of achieving organizational objectives in four areas, i.e., strategy, operations, reporting, and compliance, in the spirit of preventing disasters and maximizing entity value (Beasley et al, 2004; Quinn, 2006), as it is also built on the foundation laid by SOX (De Loach, 2003; Hirth, 2005; Moeller, 2007).

No precise recipe or silver bullet is possible in ERM implementation because so much of the process depends on organizational variables (Walker, Shenkir & Barton, 2002). Many publications have discussed based on the dynamics of the COSO Cube and have

highlighted the nuances and subtleties of the COSO ERM framework. A number of studies and prophecies (Lam, 2003) have concluded that ERM manages all business risks using an integrated and holistic approach (Mc Namee, 2004; Miccolis et al, 2003) by considering a portfolio of risks (Ching, 2007; Niehaus et al, 2004). ERM seeks to strategically consider the interactive effects of various risk events with the goal of balancing an enterprise's portfolio of risks to be within the stakeholder's appetite for risk (Beasley et al, 2007). The need for additional research has been identified by Stulz et al (2006) in their studies with respect to implementation of ERM and its metrics.

While there has been some research on the general key components of the COSO ERM framework, there is little that has been written about the approach to link the trinity forces, 'risks, objectives & corporate strategy'; and its level of transparency (Ward, 2006) within entities. Most of the studies acknowledge that the goal of ERM is to create, protect, and enhance shareholder value by managing the uncertainties surrounding the achievement of the organization's objectives (Moody, 2005), but lacks practical advice in terms of its implementation (Tueten, 2005). As risks affect entities holistically, they need to be managed in a holistic manner beyond disciplinary boundaries (Sobel & Reding, 2004). A framework of ERM should include such an approach to risk management, which provides a common understanding across a multidisciplinary group of people (Sobel & Reding, 2004) and show possible future exposures to risk (Mc Name, 2004). However, these studies have not shed light on the parameters which affect the efficiency and effectiveness of the ERM system (Berlin, 2004; Walker & Shenkir, 2006; Lewis, 2005; Marie et al, 2007; Blanco & Regan, 2006) and also on the approach to implement such a system, especially in the oil & gas sector, expressing the location of the ERM maturity level along the risk continuum (Walker & Shenkir, 2007).

The growing importance of ERM has been reflected in major publications issued by professional organizations around the world. Some studies within the banking and insurance sectors (Nagumo & Barnaby, 2006) have even expanded beyond ERM implementation by exploring the opportunities for integrating ERM (Walker, 2006) to today's ubiquitous management tools like Strategic Planning, Balanced Scorecard, TQM and Six Sigma. It is evident that ERM will continue to grow in importance and

acceptance as businesses cope with the harsh and sometimes devastating risks they confront. However, some authors have highlighted the fact that 'Risk' means differently for various people and it depends on the industry and the background they originate from (Renn, 1992; Zinn, 2006). ERM interests a wide range of professionals including actuaries, financial managers, underwriters, accountants, internal auditors, risk managers, etc. However, current ERM solutions often do not cover all risks because they are motivated by the core professional ethics and principles of those who drive forward ERM systems and their professional background. Just as 'Risk' mean differently, relationship between Corporate Governance and ERM is also a nebulous topic (Anderson & Chapman, 2002). However, it remains a matter of serious concern that there is no study or research model designed for evaluating the operational and technical challenges faced by oil & gas companies to implement such a system. Furthermore, there is no study which has identified the drivers to ERM implementation in the oil & gas companies which is facing unprecedented challenges (Ballou & Heitger, 2005; Lewis et al, 2005; Blanco & Regan, 2006).

Current status of ERM in business organizations in Dubai have been studied (Marie & Rao, 2007), but the contentious assumption is that the business climate in the UAE in general, and Dubai in particular, is similar to that in other countries globally. UAE is a Sheikhdom with no superior corporate governance attributes comparable in the global business landscape. Furthermore, the study does not fully add much credence to this academic study as it is not focused at the oil & gas companies, which are all unique as national companies dealing with sovereign assets in a strategic industry (Broomley, 1991).

Although ERM is an Anglo-Saxon phenomenon and to a degree Australasian (Merrifield, 2001; Leech, 2006), entities in other countries seem to have embraced ERM system and focused on COSO ERM implementation (Lam, 2006). Its overreaching nature appears overwhelming for some organizations (Ballou & Heitger, 2005) and yet there are no studies that exist by ***'exploring the business environment for better implementation of ERM system in the Middle East oil & gas companies'***, investigating the extent to which

these entities manage risks in a truly holistic manner. This study attempts to fill this gap by exploring the following research questions:

(1) What is the understanding of the nature of ERM within the oil industry?
(2) What are the value drivers to develop ERM in the oil companies?
(3) How do oil companies structure ERM for effective implementation?
(4) What challenges do oil companies face in implementing ERM?
(5) How do oil companies measure the performance of ERM?

----------END OF CHAPTER-2----------