Enterprise Risk Management

Index

Enterprise Risk Management – An Introduction

With the large number of corporate scandals rocking the corporate world with the turn of the century, the concept of enterprise risk management has gained immense importance.

An enterprise can be defined as any purposeful organisation or any undertaking created for business venture.

As the name suggests, enterprise risk management refers to methods and processes used by organizations to manage risks (or seize opportunities) related to the achievement of their objectives. Enterprise risk management covers all categories and all material risk factors that can influence the organization's value.

The risk based approach integrates the concepts of strategic planning, operations management and internal control.

While the traditional risk management is more about preventing something from happening, enterprise risk management is about helping something happen.

The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 defines ERM as:

"*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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*"

The COSO ERM Framework has eight Components and four objectives categories. It is an expansion of the COSO Internal Control-Integrated Framework published in 1992 and amended in 1994. The eight components are:

1. Internal Environment
2. Objective setting
3. Risk identification
4. Risk assessment
5. Risk response
6. Control activities
7. Information And communication
8. Monitoring

The Risk and Insurance Management Society, Inc. (RIMS) [RIMS Risk Maturity Model for ERM, Nov 2006] defines ERM as

the culture, processes and tools to identify strategic opportunities and reduce uncertainty. ERM is a comprehensive view of risk from both operational and strategic perspectives and is a process that supports the reduction of uncertainty and promotes the exploitation of opportunities.

Risk response

Management selects a *risk response strategy* for specific risks identified and analyzed, which may include:

1. Avoidance: exiting the activities giving rise to risk
2. Reduction: taking action to reduce the likelihood or impact related to the risk
3. Share or insure: transferring or sharing a portion of the risk, to reduce it
4. Accept: no action is taken, due to a cost/benefit decision

Monitoring is typically performed by management as part of its internal control activities, such as review of analytical reports or management committee

meetings with relevant experts, to understand how the risk response strategy is working and whether the objectives are being achieved.

ERM integrates risk into an institution's strategic plans with the goal of achieving an appropriate balance of risk and return.

ERM benefits include improved communication on risk among the senior management and others which leads to more informed decisions, better allocation of resources, and stronger governance practices.

Enterprise Risk Management provides several tiers for evaluation of risks at increasingly granular levels which risks are most significant and which mitigation activities have the most "bang for the buck" in terms of impact, likeliness and effectiveness. These levels of increasing granularity include entity, business unit, process, account and mitigation activities. Evaluations at each level filter out appropriate low risk threats based on consistent and objective criteria.

The "top-down, risk-based" approach of Enterprise Risk Management empowers managers to use their expertise to address risks not only to financial reporting but also take into consideration the strategic, security and business continuity aspects as well. For example, entity wide control evaluations can be turned from a required "check box" activity to a real linkage with process based activity level controls to help management understand the connection between principles and action.

In the ERM approach, mitigating activity becomes a strategic activity in support of corporate objectives and brings an agility that is a competitive advantage to early adopters. In this way, this new guidance paves the way not only for the reduction of external audit fees, but also to right size the resources applied to testing and documentation as well as take business value added activities into scope at the same time.

Enterprise risk management is also referred to as integrated risk management or holistic risk management or global risk management.

Evolution of enterprise risk management

In the 1970 and 80's risk management started to gain momentum having derived its origins from the insurance industry. Its early focus was on protecting against catastrophe and evolved to protecting unaffordable potential losses. Insurers found that their results were enhanced by encouraging customers to exercise reasonable care and by rewarding good performance. And so risk management evolved from natural intuition and analytical thinking into a more formal process of communication of the controls in place to influence outcomes.

In the 1980s total quality management became accepted as a means for improving the quality of business processes. Today risk management is accepted as a means of protecting the bottom line and assuring long term performance.

Risk management has become a universal management process involving quality of thought, quality of process and quality of action.

There were and still are many different approaches and methods of analysing and managing risk. In the early 1990s a risk management standard was developed in Canada. In 1995 a pre-eminent group of leading business thinkers developed the Australian and New Zealand Standard for risk management - AS/NZS 4360:1995. This standard has received a wide degree of international interest and is widely used as a guideline for implementing risk management.

The increased level of focus and formalisation of risk management as a business process has created the opportunity for experienced practitioners and innovative thinkers to capitalise on the latest technology and break new barriers in developing business solutions.

Although insurance is still widely used, larger organisations have reduced their reliance on more conventional arrangements as managers discovered that insurance did not meet all organisational needs or that internal activities could control the impact of risk and uncertainty on the organisation.

Technical and financial sides of risk management have gradually been integrated under the same independent function; most medium-size and large organisations have now adopted risk management practices because of their benefits and/or legislation compliance. While risk management practices are beginning to evolve and move away from the traditional insurance based solutions, the regulatory requirements are also on the rise. Compliance with these regulatory requirements requires establishment of internal measures and controls that must be documented as well as monitored and tested regularly. The establishment of an enterprise risk management framework is thus the need.

The general factors that gave birth to Enterprise Risk Management as a separate area of practice are:

1) Increase in complicated risks
2) External pressures – customers, suppliers, employees and others
3) Increasing tendency towards an integrated view of risks
4) Growing tendency to quantify risks
5) Sharing of common Enterprise Risk Management practices and tools amongst various organizations
6) Organizations have come to relies the optimistic side - the value creation potential of risk
7) Increasing stakeholder pressure and regulatory requirements

Its history can be traced as follows:

1974	Basel Committee on Banking Supervision
1988	Basel Capital Accord setting forth a new framework for minimum risk based Capital requirements (Basel II in 2004)
1985	COSO was formed to sponsor the National Commission on Fraudulent Financial Reporting, an independent commission to undertake a private sector study of factors that caused fraudulent financial reporting. The COSO framework developed set forth recommendations for internal controls needed to identify and monitor risks.
1992	Following a series of high profile corporate frauds and accounting scandals, the London Stock Exchange introduced new regulations covering various aspects of Corporate governance such as, who could be a director, what committees the Board of directors should have, and what steps they should take to ensure their company's accounts could be relied on and their assets were safeguarded.
1995	Development of national standards on Risk Management began with Aus/NZ Risk Management Standard creating a generic framework for the risk management process as part of an organization' culture. Similar standards in Canada (Dey Report 1997) and Japan, and in the UK (2000)
1996	NAIC (National Association of Insurance Commissioners in United States) introduced risk based capital requirement for insurance companies.
2002	A string of corporate accounting scandals has profound implications in the US and worldwide and led to the passage of Sarbanes-Oxley Act

2004	COSO Enterprise Risk Management Integrated Framework

The importance of ERM

Risk management is not new. The concept has been around in investment, banking, insurance, artificial intelligence, and public policy processes. Risk Management has become relevant to all aspects of management, governance and professions.

Risk Management is all about unidentified risks that can pose a major threat to an enterprise or result in significant opportunities being missed. Frequently just after a failure, loss, blunder or catastrophe we discover in hindsight that the facts have been staring us all along in the face, but they have been either ignored or overlooked. This could be because of:

1) Overestimation - a determination to overemphasize information, leading to a false conclusion.

2) Underestimation - business analysts or leadership completely misreads a competitor's intentions or market event.

3) Over-confidence - bad assumptions based on our own certainty on how we would handle the situation.

4) Complacency - something is going to happen, though not sure what or when, and yet no action is taken.

5) Ignorance - When there is virtually no intelligence, we are at the mercy of events.

6) Failure to join the dots - failure to make connections between bits of intelligence to make a coherent whole.

Enterprise Risk Management is a proven framework to systematically address these weaknesses.

Technology and process are seen as key drivers in a race against time to establish new means of competitive edge and differentiation of services. Interactive systems can now harness the incredible intuition of the human mind to model complex risk solutions.

Enterprise risk management highlights not only the high frequency risks, but also the low frequency high impact risks. 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. Enterprise Risk Management 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. Enterprise Risk Management 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. With ERM, management can prioritize the full costs versus the benefits to make a better decision.

Organizations that have adopted ERM early are way ahead of others. They make rationalized investments in risk management and are proactive in optimizing their risk profiles.

Every enterprise exists with the objective of realizing value for its stakeholders. Value is created, preserved or eroded by management decisions in all activities, from setting strategy to operating the enterprise. ERM supports value creation by enabling management to deal effectively with potential future events that create uncertainty and respond in a manner that reduces the probability of downside outcomes and increases the upside.

The objectives of an ERM framework are:

- Improve risk-based decision making
- More effective use of capital
- Comply with regulatory changes
- Improve shareholder value
- Anticipating problems before they become a threat
- Co-coordinating various risk management activities

ERM helps an enterprise protect risks and enhance value in three ways:

1. focus on establishing sustainable competitive advantage – ERM integrates the varying views of risk and enables the enterprise to successfully respond to changing environment. Risk management is applied to all levels and all sources of enterprise value, not just physical and financial ones.
2. optimizing the cost of managing risk – ERM helps management aggregate risk acceptance and transfer decisions, eliminate redundant activities and determine the level of acceptable risk.
3. helping management improve business performance – ERM reduces unacceptable performance variability and loss exposure by anticipating the impact of major events and developing responses to prevent those events from occurring

ERM is fast becoming the best practice standard because the traditional approach of managing risks has not produced effective results. Traditionally, risk management was highly fragmented in its approach, which has been proved to be ineffective over time. It does not work because risks are highly interdependent and cannot be segmented and managed solely by independent units.

Other reasons for the increasing importance of ERM are:

1. internal demand – actual crises or losses followed by critical assessments by auditors and regulators tend the top management to question the effectiveness of the internal control environment and the adequacy of risk reporting. This introspection often leads to the emergence of a risk leader who promotes a program for the development of an effective ERM framework.
2. external developments – the increasing concerns of the institutional investors and analysts about the risk exposures facing an organization, and of the regulators on all aspects of risks during examination and ascertaining the role of the senior management in the risk management process can be allayed with more effective risk management and disclosure of enterprise wide risks. Further, the availability and liquidity of new risk transfer products such as credit derivatives and catastrophe bonds allow the end user to select which risks to retain and which risks to hedge.
3. advances in risk methodologies and tools – over the past several years volatility based models such as value-at-risk (VaR) and return-on-risk-adjusted-capital have been applied to measure and manage all types of market risk within an organization. These models have been applied to default and portfolio management models and also credit risk management.

Organizations that have adopted the ERM framework have experienced an increase in shareholder value, reduction in losses and earnings volatility, and general improvement in the measurement and management of overall risks.

ERM:

1. supports strategic and business planning
2. prepares the enterprise for quick grasp of opportunities
3. reduces uncertainty in business
4. enables better service delivery and more efficient use of resources
5. helps focus internal audit programme
6. existence of an ERM framework reassures stakeholders
7. promotes continual development

Inherent Limitations of Enterprise Risk Management

ERM, no matter how well designed and operated can provide only reasonable assurance to management and the Board of directors regarding achievement of the entity's objectives.

The inherent limitations include the following:

- Faulty human judgment in decision making
- Breakdowns caused by human failures such as a simple error or mistake
- Controls circumvented by the collusion of two or more people
- Ability of Management to override the ERM process
- Need to consider the relative costs and benefits of risk responses.

- The complexity of the process deter many from accepting an integrated framework and many end up with risk management solutions for some specified areas only, which is against the very concept of enterprise risk management

While ERM is emerging as the best practice model for measuring and managing all types of risks across the enterprise, the key challenges faced by organizations adopting the ERM framework are:

- Defining the role of the credit risk officer
- Establishing the ERM framework
- Developing the risk technologies, including internet or intranet applications
- Implementing operational risk management
- Determining the role of new transfer products

Ineffective risk management can lead to adverse publicity, falling earnings and stack prices, and even bankruptcy.

Technological needs

One of the key challenges within the risk, performance, compliance and business continuity areas of the corporation is the management of data in spreadsheets and other office files, often referred to as unstructured data. Not only do spreadsheets lack the authentication, audit trail, and integrity, but they also lack accessibility to roll-up information into an enterprise wide picture. This is a critical barrier to systematically identify dependencies and track change. Information within spreadsheets is largely inaccessible to infrastructure tools like business intelligence, content management and business process management functionality and the cost of maintenance of this data is unreasonable. The

presence of spreadsheets is a symptom of manual processes which are also typically both expensive and error prone.

This necessitates the existence of an Enterprise Risk Management solution. One of the core value propositions of an ERM solution is to effectively solve this problem of collecting and managing unstructured risk and performance data. A robust ERM solution should provide a schema or organizational hierarchy for risk data so that ERM can bring together unstructured and structured data across the enterprise with the goal to improve decision making. This framework for organizing data provides the foundation for increased quality and efficiency for assessments as well as a process for aggregation and analysis of the information for dependencies.

A comprehensive technological solution, addressing key ERM processes in an integrated fashion has to be developed. This is not only a costly and time consuming process, but a common solution for all is difficult to develop, given the varied needs of each enterprise.

The Enterprise Risk Management process

The following steps illustrate the various stages in the risk management process.

1. Establish Context –

This step includes establishing External, Internal and Risk Management Contexts.

The External Context starts with a definition of the relationship of the enterprise with its environment, including identification of the enterprise's strengths, weaknesses, opportunities, and threats ("SWOT analysis"). This context-setting

also identifies the various stakeholders (shareholders, employees, customers, community), as well as the communication policies with these stakeholders.

The Internal Context starts with an understanding of the overall objectives of the enterprise, its strategies to achieve those objectives and its key performance indicators. It also includes the organization's oversight and governance structure.

The Risk Management Context identifies the risk categories of relevance to the enterprise and the degree of coordination throughout the organization, including the adoption of common risk metrics.

One should identify the major activities, processes and functions of the enterprise and categorize and prioritize such activities.

2. Identify Risks

Event identification involves identifying potential events either from internal or from external sources that affect the achievement of objectives.

A) Internal factors include:

a) Infrastructure i.e. availability of assets, capability of assets, Access to capital, complexity.

b) Personnel i.e. Employee capability, Fraudulent activity, Health and safety

c) Process i.e. capacity, design, Execution, suppliers/ dependencies

d) Technology i.e. Data integrity, data and system availability, development, deployment and maintenance.

B) External Factors include:

a) Economic factors such as capital availability, credit, financial markets, unemployment, competition

b) Natural Environment such as Emissions and waste, energy, Natural disaster

c) Political changes such as changes in Government, legislations, public policies, Regulations`

d) Social factors such as Demographics, Consumer behavior, corporate citizenship, privacy, terrorism

e) Technological changes such as Interruptions, External data, emerging technology

Since events do not occur in isolation, it is important that the management understands how events relate to one another. By assessing the relationship, they can determine where risk management efforts can be best directed.

Risk identification can start with the source of problems, or with the problem itself.

Source analysis Risk sources may be internal or external to the system that is the target of risk management. Examples of risk sources are: stakeholders of a project, employees of a company

Problem analysis Risks are related to fear. For example: the fear of losing money, the fear of abuse of privacy information or the fear of accidents and casualties. The fear may exist with various entities, most important with shareholder, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated.

For example: stakeholders withdrawing during a project may endanger funding of the project or privacy information may be stolen by employees even within a closed network

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event.

Common risk identification methods are:

a) Objectives-based Risk Identification Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.

b) Scenario based Risk Identification In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk.

c) Taxonomy-based Risk Identification The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.

d) Common-risk checking In several industries lists with known risks are available. Each risk in the list can be checked for application to a particular situation.

3. Analyze and Quantify Risks

This step involves calibrating and, wherever possible, creating probability distributions of outcomes for each material risk. This step provides necessary input for subsequent steps, such as integrating and prioritizing risks. Analysis techniques range along a spectrum from qualitative to quantitative, with sensitivity analysis, scenario analysis, and/or simulation analysis applied where appropriate.

4. Integrate Risks

This step involves aggregating all risk distributions, reflecting correlations and portfolio effects, and expressing the results in terms of the impact on the enterprise's key performance indicators (i.e., the "aggregate risk profile").

5. (A) Risk assessment

Once the risks are identified, they should be assessed as to their potential severity of loss and to the probability of occurrence. The impacts should be examined individually or by category across the entity. Risks are assessed on both an inherent and residual basis.

i. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the likelihood or impact of the risk
ii. Residue risk is the risk that remains after management's response to the risk.

Risk assessments are conducted to estimate how much damage or injury can be expected from exposures to a given risk agent and to assist in judging whether these consequences are great enough to require increased management or regulation.

The techniques of risk assessment are:

1. Qualitative techniques
    a. Questionnaire.
    b. Survey
    c. Interviews, etc.
2. Quantitative techniques
    a. Probability based techniques
    b. Back testing.
    c. Non Probabilistic Techniques
    d. Sensitivity Analysis.
    e. Scenario Analysis.
    f. Stress Testing.
    g. Bench Marking

The methods and sequence of steps involved in conducting a risk assessment vary with the kind of risk and its possible consequences. However, in its most general form, the process consists of a *source assessment*, an *exposure assessment,* an *effects assessment*, and is normally concluded by an integrative *risk characterization*.

a) Source assessment seeks to identify and evaluate the sequences of events through which an exposure to a risk could arise. In risk assessments of engineering systems, for example, this can be a particularly extensive and detailed exercise—such as evaluating the possibility that a pump in a manufacturing operation might fail, leading through a series of steps to increased levels of toxic substances on the shop floor. Alternatively, this kind of analysis might be aimed at finished products, whose physical features along with typical use patterns could result in safety hazards.

b) Exposure assessment seeks to determine the areas exposed to a risk, along with the magnitude, duration, and timing of their exposures. Depending on the needs of the analysis, the evaluation might focus on current, past, or future exposures.

c) Effects assessment determines the extent of adverse effects likely to result from given levels of exposure to a risk. For resource and efficiency reasons, this kind of analysis is usually conducted in stages. The initial analytical step is to determine if exposures to a risk at any level could cause adverse effects. Then a more detailed study is conducted to determine what quantitative relationship (dose–response) exists between the level of exposure and the incidence of adverse effects.

d) Risk characterization is the concluding step of a risk assessment. This is an important integrative task, which involves assembling the prior analysis components into a bottom-line picture of the nature and extent of the risk. The principal topics include the kinds of effects likely to arise, the risk's potency (i.e., the severity of the adverse effects), the areas affected, the likelihood of exposure, and the risk's ultimate magnitude (i.e., potency adjusted for the likelihood of exposure). Risk characterizations are usually the principal means through which a risk assessment's findings are communicated to risk managers, policy makers, journalists, and the public.

It is generally acknowledged that characterizations need to provide deeper insight into how risk estimates and findings are generated (including a discussion of the assumptions that underlie the calculations). In addition, characterizations should consider a range of plausible risk estimates (which could result from the use of plausible alternative assumptions or differing models of exposure and response relationships) and should more clearly discuss

the uncertainties and limitations in the empirical data on which the risk assessment is based.

(B) Risk Measurement

A. Solvency-related measures:-These measures concentrate on the adverse "tail" of the probability distribution and are relevant for determination of capital requirements. They are of particular concern to customers and their proxies, e.g., regulators and rating agencies.

1. Probability of ruin:-The percentile of the probability distribution corresponds to the point at which capital is exhausted. Typically, a minimum acceptable probability of ruin is specified, and economic capital is derived there from.
2. Shortfall risk:-The probability that a random variable falls below some specified threshold level. (Probability of ruin is a special case of shortfall risk in which the threshold level is the point at which capital is exhausted.)
3. Value at risk (VaR):- The maximum loss an organization can suffer, under normal market conditions, over a given period of time at a given probability level (technically, the inverse of the shortfall risk concept, in which the shortfall risk is specified, and the threshold level is derived therefrom). VaR is a common measure of risk in the banking sector, where it is typically calculated daily and is used to monitor trading activity.
4. Economic cost of ruin (ECOR):-An enhancement to the probability of ruin concept (and thus shortfall risk and VaR) in which the severity of ruin is also reflected. Technically, it is the expected value of the shortfall. (In an analogy to bond rating, it is comparable to considering the salvage value of a bond in addition to the probability of default.) For insurance companies, the equivalent term is expected policyholder deficit (EPD),

and represents the expected shortage in the funds due to policyholders in the event of liquidation.

5. Tail Value at Risk (Tail VaR) or Tail Conditional Expectation (TCE):-An ECOR-like measure in the sense that both the probability and the cost of "tail events" are considered. The calculation differs from ECOR in such a way that it has a desirable statistical property (i.e., coherence) that is beyond the scope of this document to describe.

B. Performance-related measures:-These measures concentrate on the mid-region of the probability distribution i.e., the region near the mean, and are relevant for determination of the volatility around expected results. They are of particular concern to owners and their proxies, e.g., stock analysts:

1. Variance—the average squared difference between a random variable and its mean.
2. Standard deviation—the square root of the variance.
3. Semi-variance and downside standard deviation—modifications of variance and standard deviation, respectively, in which only unfavorable deviations from a specified target level, are considered in the calculation.
4. Below-target-risk (BTR)—the expected value of unfavorable deviations of a random variable from a specified target level.
5. Covariance—a statistical measure of the degree to which two random variables are correlated. Related to correlation coefficient (correlation coefficient is covariance divided by the product of the standard deviations of the two random variables). A correlation coefficient of +1.0 indicates perfect positive correlation; -1.0 indicates perfect negative correlation (i.e., a "natural hedge"); zero indicates no correlation.
6. Covariance matrix—a two-dimensional display of the covariance (or correlation coefficients) among several random variables; the covariance between any two variables is shown at their cross-section in the matrix.

(C) Risk Modeling

Risk modeling refers to the methods by which the risk and performance measures described above are determined.

1. Analytic methods use models whose solutions can be determined "in closed form" by solving a set of equations. These methods usually require a restrictive set of assumptions and mathematically tractable assumed probability distributions. The principal advantage over simulation methods is ease and speed of calculation.
2. Simulation methods (often called Monte Carlo methods) use models that require a large number of computer-generated "trials" to approximate an answer. These methods are relatively robust and flexible, can accommodate complex relationships (e.g., so-called path dependent relationships commonly found in options pricing), and depend less on simplifying assumptions and standardized probability distributions. The principal advantage over analytic methods is the ability to model virtually any real-world situation to a desired degree of precision.
3. Statistical methods use models that are based on observed statistical qualities of (and among) random variables without regard to cause-and-effect relationships. The principal advantage over structural models is ease of model parameterization from available (often public) data.

   Mean/variance/covariance (MVC) methods are a special class of statistical methods that rely on only three parameters: mean, variance, and covariance matrix.

a) Structural methods use models that are based on explicit cause-and-effect relationships, not simply statistical relationships such as correlations. The cause/effect linkages are typically derived from both data and expert

opinion. The principal advantages over statistical methods include the ability to examine the causes driving certain outcomes (e.g., ruin scenarios) and the ability to directly model the effect of different decisions on the outcome.

b) Dynamic Financial Analysis (DFA) is the name for a class of structural simulation models of insurance company operations, focusing on underwriting and financial risks, designed to generate financial pro forma projections.

6. Prioritize risk factors

The resulting list of risk factors (typically several dozen long at this stage) is not yet useful or actionable, although each factor has passed the materiality screen. It now requires prioritizing.

There are two principal methods of comparing risks in order to rank and prioritize risk factors.

a) Specific risk comparison refers to side-by-side evaluation of the risk (on an absolute or relative basis) associated with exposures to a few substances, products, or activities. Such comparisons may involve similar risk or widely different risks.

b) Programmatic comparative risk assessment, which seeks to make macro-level comparisons among many widely differing types of risks, usually to provide information for setting regulatory and budgetary priorities for hazard reduction. In this kind of comparison, risk rankings are based on the relative magnitude of risk (which hazards pose the greatest threat) or on relative risk reduction opportunities (i.e., the amount of risk that can be avoided with available technologies and resources).

7. Treat/Exploit Risks –

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

a) Acceptance (Retention)
b) Avoidance
c) Reduction (Mitigation)
d) Transfer

Ideal use of these strategies may not be possible. Some of them may involve trade offs that are not acceptable to the organization or person making the risk management decisions.

a) Risk Acceptance

This involves accepting the loss when it occurs. Self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured are retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is

different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

b) Risk avoidance

This includes not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning the profits.

c) Risk reduction

This involves methods that reduce the severity of the loss by:

1. Diversifying product offerings.
2. Establishing operational limits.
3. Establishing effective business processes.
4. Enhancing management involvement in decision-making, monitoring.
5. Rebalancing portfolio of assets to reduce exposure to losses.
6. Reallocating capital among operating units.

d) Risk transfer

This means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking

offsetting positions in derivatives is typically how firms use hedging to manage financial risk.

8. Inform /Communicate

Information is needed at all levels of organization to identify, assess, and respond to risks, and to otherwise run the entity and achieve its objectives. Information both from internal and external sources is obtained and analyzed in setting strategy and objectives, identifying events, analyzing risks, determining risk responses, and otherwise effecting enterprise risk management and carrying out other management activities. A broad based, generic depiction of information flows into, out of, and within an entity to support its ongoing management. The design of the information system depends on:

- Entity's approach to E.R.M and its degree of sophistication
- Types of events affecting the entity.
- Entity's overall information technology architecture.
- Degree of centralization of supporting technology

Management provides specific and directed communication that addresses behavioral expectations and the responsibilities of personnel. This includes a clear statement of the entity's risk management philosophy and approach and a clear delegation of authority.

9. Monitor and review

This step involves continual gauging of the risk environment and the performance of the risk management strategies. Monitoring could be through on going monitoring activities or separate evaluations. The frequency of separate

evaluations depends on the assessment of risks, and the effectiveness of the on going ERM. Monitoring also provides a context for considering risk that is scalable over a period of time (one quarter, one year, five years). The results of the ongoing reviews are fed back into the context-setting step and the cycle repeats.

An effective risk management program will ensure that essential information is available to make informed decisions.

Implementation of Enterprise Risk Management Program

ERM provides a company with the process it needs to become more anticipatory and effective at evaluating, embracing and managing the uncertainties it faces as it creates sustainable value for stakeholders.

The establishment of a framework requires the following:

- Clear statement of company's objectives
- Identification process
- Risk policies – (Definition of risk, responsibility, risk appetite and review period)
- Reporting lines – (who is to report to whom)
- Data collection process
- Risk evaluation methods – (the methods could be Stress/scenario testing, Stochastic modeling, Traffic light, etc.)

The basic elements of an effective risk management program are:

1. Education – Acquiring or developing an enterprise risk management program should be followed by education and training. The entire

organization must know and understand the policies, procedures and objectives laid down. Training of employees must be an ongoing process.

2. Commitment at the top - Senior management and Board of Directors should have commitment for a broad-based, strategic risk management process. This commitment must be sufficient to ensure that risk management becomes a core skill of the company and is practiced throughout the organization, particularly at the operating level.
3. Documentation - Risk management policies and procedures must be established in writing for the most prominent risks, with specific objectives and targets. Due diligence requires documentation to prove that procedures are not only established but adhered to.
4. Accountability – A sense of responsibility must be instilled throughout the organization. Everybody should understand that risk management is everyone's job. There should be clearly defined responsibilities for managing and controlling risk. Performance evaluations which include specific risk management objectives assure accountability. Effecting a culture of change from top to bottom regarding the importance of managing and mitigating risk every day will have a positive impact at all enterprise levels.
5. Transparency – The organization must be able to clearly demonstrate the processes and controls, and provide audit trails, tests and reports to validate results.
6. Adequate resources and tools focused on the most prominent risks should be made available so that compliance and effective performance is assured.
7. Continuous process – Individual processes of the ERM program must be repeatable. Identifying, measuring, managing and monitoring risks should be an ongoing process for continuous evaluation and action for the

enterprise. New needs should be continuously looked for and new services created for the emerging needs.

8. Testing and monitoring of all programs and procedures, particularly emergency and business recovery plans with continual improvement as the goal should be carried out.
9. Collaboration – It should be made clear that enterprise risk management cuts across all departmental and geographical boundaries. What happens in one department (area) of an enterprise has a ripple effect throughout the organization, and an overall impact on risk at the enterprise level. A collaborative effort is required with each employee playing his part with the understanding of the interdependencies of the overall strategy.
10. Regular reports including independent audits should be prepared for review by senior management and board directors. These reports must provide concise information regarding the status (including deficiencies) of all corporate risk management programs.
11. Integration – Enterprise risk management should be integrated into company culture and all decision making – capital allocation, pricing, or any strategic decision.

The establishment of an effective framework starts with a focus on regulatory related risks and compliance requirements, and gradually moves to broader proactive risk identification, with action plans to mitigate and manage those risks. Cost is always a factor to be considered. However, once processes are set to measure risk in the same context as opportunity, the ROI considerations in deciding to adopt ERM are easier to justify.

While the following steps provide a simplified view of the task of implementing ERM, the implementation process does not occur overnight and, for certain, is not easy to accomplish. ERM is a journey and these steps are a starting point.

1. Organizational design of business
2. Create an enterprise risk management organization
3. Establishing an ERM organization
4. Performing risk assessments
5. Determining overall risk appetite
6. Identifying risk responses
7. Communication of risk results
8. Advance the risk management capability of the organization for one or two priority risks
9. Evaluate the existing ERM infrastructure capability and develop strategy for advancing it
10. Advance the risk management capabilities for key risks
11. Optimizing the return on risk management investments
12. Leveraging risk management
13. Monitoring
14. Oversight & periodic review by management

STEP 1: organizational design of business

- Strategies of the business
- Key business objectives
- Related objectives that cascade down the organization from key business objectives
- Assignment of responsibilities to organizational elements and leaders (linkage). For example,
    - Mission – To provide high-quality accessible and affordable community-based health care

- Strategic Objective – To be the first or second largest, full-service health care provider in mid-size metropolitan markets
- Related Objective – To initiate dialogue with leadership of 10 top under-performing hospitals and negotiate agreements with two this year

STEP 2: Create an enterprise risk management organization

The program should start with the appointment of a chief risk officer and formation of an enterprise risk management committee. The committee is responsible for directing all credit, market and operational risk management activities, as well as coordinating oversight units such as insurance, security, audit and compliance. The ERM organization may report to the CEO or the CFO and should have a direct reporting relationship to the senior management.

STEP 2: Articulate the risk management vision and support it with a compelling value proposition.

The "risk management vision" is a shared view of the role of risk management in the organization and the capabilities desired to manage its key risks.

"Risk management capabilities" include the policies, processes, competencies, reporting, methodologies and technology required to execute the organization's response to managing its priority risks. They also consist of what we call "ERM infrastructure."

Defining the specific capabilities around managing the priority risks begins with prioritizing the critical risks and determining the current state of capabilities around managing those risks. Once the current state of capabilities is determined for each of the key risks, the desired state is assessed with the objective of

identifying gaps and advancing the maturity of risk management capabilities to close those gaps.

Examples of elements of ERM infrastructure include, among other things, an overall risk management policy, an enterprise-wide risk assessment process, presence of risk management on the Board and CEO, a chartered risk committee, clarity of risk management roles and responsibilities, dashboard and other risk reporting, and proprietary tools that portray a portfolio view of risk.

The greater the gap between the current state and the desired state of the organization's risk management capabilities, the greater the need for ERM infrastructure to facilitate the advancement of those risk management capabilities over time. A working group of senior executives should be empowered to articulate the role of risk management in the organization and define relevant goals and objectives for the enterprise as a whole and its business units.

STEP 3: Establish ERM

1. Establish an integrated risk management framework to measure and manage all aspects of risk.
2. Determine a risk philosophy
3. Survey risk culture
4. Consider organizational integrity and ethical values
5. Decide roles and responsibilities

STEP 4: Assess risks

Risk assessment is the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed. Risk analysis involves:

- Identification
- Measurement
- Prioritization

STEP 5: Determine risk appetite

Risk appetite is the amount of risk — on a broad level — an entity is willing to accept in pursuit of value. Use quantitative or qualitative terms (e.g. earnings at risk vs. reputation risk), and consider risk tolerance (range of acceptable variation). Risk tolerance is the acceptable level of variation relative to the achievement of objectives

Key questions are:

- What risks will the organization not accept? *(e.g. environmental or quality compromises)*
- What risks will the organization take on new initiatives? *(e.g. new product lines)*
- What risks will the organization accept for competing objectives? *(e.g. gross profit vs. market share?)*

STEP 6: Identify risk responses

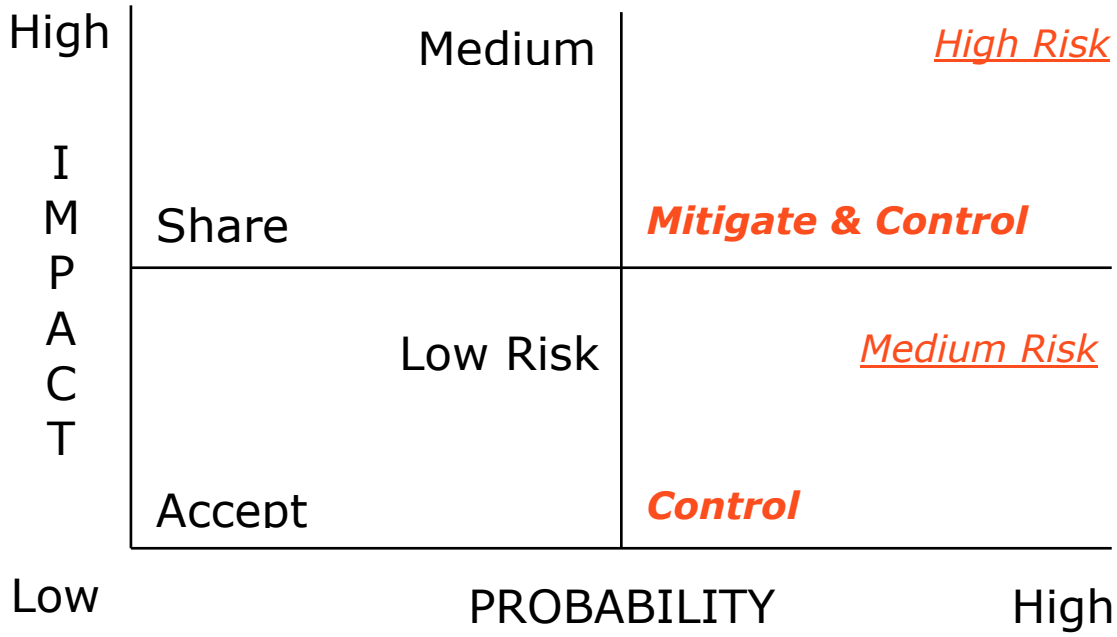
The risk exposure should be quantified. While managing risks, the following options are available:

- Accept (monitor)
    - "Self-insuring" against loss
    - Relying on natural offsets within a portfolio.
    - Accepting risk as already conforming to risk tolerances
- Avoid (eliminate / get out of situation)

        - Disposing off a business unit, product line, geographical segment.
        - Deciding not to engage in new initiatives/activities that would give rise to the risks
- Reduce (institute controls)
        - Diversifying product offerings
        - Establishing operational limits.
        - Establishing effective business processes.
        - Enhancing management involvement in decision-making, monitoring.
        - Rebalancing portfolio of assets to reduce exposure to losses.
        - Reallocating capital among operating units
- Share/transfer (partner with someone)
        - Insuring significant expected losses
        - Entering into Joint venture/ Partnership
        - Entering into syndication agreements.
        - Hedging risks.
        - Outsourcing Business processes.
        - Sharing risks through contractual agreements

- Residual risk – this risk is the unmitigated risk – e.g. shrinkage.

The option taken is based on the probability of occurrence and the impact on the enterprise. The following diagram shows impact vs. probability:



STEP 7: Communicate results

Results can be communicated through any of the following means:

- Dashboard of risks and related responses (visual status of where key risks stand relative to risk tolerances)
- Flowcharts of processes with key controls noted
- Narratives of business objectives linked to operational risks and responses
- List of key risks to be monitored or used
- Management understanding of key business risk responsibility and communication of assignments

STEP 8: Advance the risk management capability of the organization for one or two priority risks.

This step focuses the organization on improving its risk management capability in an area where management knows improvements are needed.

STEP 9: Evaluate the existing ERM infrastructure capability and develop strategy for advancing it.

ERM infrastructure facilitates three very important things with respect to ERM implementation.

1. It establishes fact-based understanding about the enterprise's risks and risk management capabilities.
2. It ensures there is ownership over the critical risks.
3. It drives closure of gaps.

ERM infrastructure is not a one-size-fits-all. What works for one organization might not work for another. The elements of ERM infrastructure vary according to the techniques and tools deployed, the breadth of the objectives addressed, the organization's culture and the extent of coverage desired across the organization's operating units. Management should decide the elements of ERM infrastructure needed according to these and other appropriate factors.

STEP 10: Advance the risk management capabilities for key risks.

This step begins with selecting the enterprise's priority risks. Once the priority risks are defined, management must decide the current state for each risk and then assess the desired state with the objective of advancing the maturity of the capabilities around managing those risks.

Risk management capabilities must be designed and advanced, consistent with an organization's finite resources. For each priority risk, management evaluates the relative maturity of the enterprise's risk management capabilities. From there, management needs to make a conscious decision: how much added capability do we need to continually achieve our business objectives? Further, what are the expected costs and benefits of increasing risk management

capabilities? The goal is to identify the organization's most pressing exposures and uncertainties and to focus the improvement of capabilities for managing those exposures and uncertainties. The ERM infrastructure management has chosen to put in place drives progress toward this goal.

STEP 11: optimizing the return on risk management investments

Risk management processes and risk transfer strategies should be linked to improve effectiveness in achieving the enterprise's risk objectives and to improve efficiency in terms of achieving those objectives at the lowest cost.

STEP 12: leveraging risk management

Risk/return considerations should be incorporated in product development and pricing, relationship management, investment and portfolio management, and mergers and acquisitions to enable making of better decisions. Risk management is not just about protecting but can also be an important tool for improving business performance.

STEP 13: Monitoring

Monitoring should be done at each process level and activity level. It involves:

- Collect and display information
- Perform analysis
    - Risks are being properly addressed
    - Controls are working to mitigate risks

STEP 14: Oversight & periodic review by management

- Accountability for risks
- Ownership

- Updates
    - Changes in business objectives
    - Changes in systems
    - Changes in processes

Problems faced by enterprises in implementation of the ERM framework

A lack of precedent, standards, and methodology in legislation leaves the situation wide open with little guidance for practical implementation of ERM. 'Enterprise Risk Management – Integrated Framework', published by the Committee of Sponsoring Organization of the Treadway Commission (COSO), provides some initial structure for such an implementation but lacks practical advice for the application of its principles. The plan is intended for application across an entire given organization, leaving business executives with a large task ahead of them requiring substantial costs and vast changes in risk management approach and method.

Hurdles involved in the implementation of enterprise wide ERM range from concrete needs such as decent software to less easily definable needs such as a paradigm shift in the minds of employees. Despite data figures that show how prevention of problems saves great amounts of money, companies have difficulty allotting funds when compared with optimistic and ignorant belief that catastrophic events won't occur. Data also shows that relatively small percentages of small and midsize companies have basic plans in place such as crisis management, business recovery, and others. Given these statistics, it is not surprising that very few companies have set into motion a true enterprise wide ERM approach.

Roles and Responsibilities of various authorities in the ERM process

Everyone in an entity has some responsibility for ERM. An organization's risk management policy should set out its approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the organization

To work effectively, the risk management process requires:

1) commitment from the chief executive and executive management of the organization
2) assignment of responsibilities within the organization
3) Allocation of appropriate resources for training and the development of enhanced risk awareness by all stakeholders.

The responsibility of the senior management is the greatest. The roles of various authorities in the ERM process are discussed as under:

Role of the Chief Risk Officer

Mostly, the Chief Risk Officer reports to the CEO/CFO and has a direct reporting relationship with the top management (Board of Directors). Heads of credit risk, market risk, operational risk, insurance and portfolio management report to the Chief Risk Officer. The Chief Risk Officer is also responsible for capital management, risk analytics and reporting, and the heads of the risk management at the business units.

He is directly responsible for:

- Providing overall leadership, vision and direction for ERM
- Establishing an integrated risk management framework for all aspects of risks across the enterprise

- Developing risk management policies, including quantification of management's risk appetite through specific risk limits
- Implementing a set of risk metrics and reports, including losses and incidents, key risk exposures, and early warning indicators
- Allocating economic capital to business activities based on risk, and optimizing the company's risk portfolio through business activities and risk transfer strategies
- Improving the risk management readiness through communication and training programs, risk based performance measurement and incentives, and other change management programs
- Developing the analytical, systems and data management capabilities to support the risk management program

Role of the risk committee

The role of the Risk committee is to:

- Participate in risk strategy analysis
- Develop and refine risk appetite/tolerance.
- Evaluate material risk exposures
- Oversee the role and responsibilities of the Internal Auditor
- Review semi-annual and annual consolidated reports

Role of the top management/ Board of directors

The Board and senior management should be fully aware of, and understand, the risks associated with the institution's business activities. They should ensure that such activities, under diverse operating circumstances, are:

- conducted in a safe and sound manner and in line with high standards of professionalism and sound business practice;
- consistent with the institution's risk management philosophy and business strategy; and
- subject to adequate risk management and internal controls

The organization must therefore have proper policies and procedures, risk measurement and reporting systems and independent oversight and control processes. Their responsibility includes:

1. Establishing policies and procedures for business activities - The Board, or an authorized senior management group, is responsible for establishing the organizational structure and comprehensive and adequate written policies and procedures for the institution's business activities, and the management of the risks inherent in these activities. These should clearly:
    i. delineate the lines of authority and the responsibilities of the Board, senior management and other personnel, including the chief risk officer for managing risk;
    ii. set out the scope of activities of each group in the institution responsible for risk management;
    iii. Identify pertinent risk management issues including, where applicable, the appropriate risk and control limits, the reporting of risk positions and performance, capital requirements, accounting treatment and standards, and investigation and resolution of irregular or disputed transactions.
2. Approval of policies – The Board should approve policies pertaining to the evaluation and management of risks. . These approved policies should cover areas such as:
    i. managerial oversight and structure;

ii. the organisation's risk appetite in terms of loss tolerance, risk-to-capital leverage, and target debt rating;
iii. Approved activities,
iv. markets and types of instruments;
v. business strategy
vi. business continuity recovery strategies; and
vii. Risk management methodologies.

3. Implementation of policies - Senior management should be responsible for implementing the policies and procedures for conducting the risk strategy and policies approved by the Board. It should ensure that the institution has effective risk management and control processes, reliable risk measurement and reporting systems, and competent staff for sound risk management.
4. Expertise – The Board needs to ensure that the organization has the required risk management skills and risk absorption capability to support its business strategy
5. Framework – The Board is responsible for implementing an integrated risk measurement and management framework for enterprise risk
6. Standards – The Board has to establish risk assessment and audit processes as well as benchmark company practices to industry best practices
7. Culture – the Board has to shape the organisation's risk culture by setting the tone from the top not only through words but actions and reinforce the commitments through incentives
8. Learning – the Board has to provide appropriate opportunities for organizational learning, including lessons from past experiences and ongoing training and development
9. Communication - The Board should also conduct and encourage discussions and communication with senior management, and between

senior management and other staff, on the institution's risk management policies and processes and risk exposures. The Board should be regularly kept informed of the institution's risk exposures, business direction and significant transactions

10. Review and monitoring - The Board should periodically
    i. Reevaluate significant risk management policies, placing emphasis on the institution's financial objectives and risk tolerance.
    ii. Review the adequacy and appropriateness of the institution's policies and procedures, and risk management processes - the methodologies, models and assumptions used to measure risk and limit exposures, performance and capital position, as well as internal control procedures
    iii. Review selected individual transactions, and the aggregate portfolio for compliance with the institution's risk strategy and policies
    iv. Deficiencies should be promptly remedied
11. Business continuity plans - Senior management should also be responsible for ensuring that business continuity plans have been prepared. These plans should be periodically reviewed and tested so that important changes in the risk environment are assessed and catered for
12. Sufficient capital - It is the responsibility of the Board and senior management to ensure that the institution maintains sufficient capital to support the risk exposures that may arise from its business activities. Hence, there should be mechanisms to inform them of significant changes in the institution's activities that would warrant a review of the adequacy of capital supporting these activities

The board provides oversight with regard to ERM by:

i. Knowing the extent to which the management has established effective ERM in the organization
ii. Knowing and concurring with entity's risk appetite
iii. Reviewing the entity's portfolio of risk and considering it against the entity's risk appetite on a regular basis
iv. Being apprised of the most significant risks and whether management is responding suitably.

Role of chief executive officer

The chief executive officer plays a key role in

- Providing direction to the senior managers
- Setting broad based policies reflecting the entity's risk management philosophy and risk appetite.

Role of management

The role played by the management is to

- Comply with risk management policies.
- Applying ERM techniques and methodologies.
- Ensuring risks are managed on daily basis
- Provide unit leadership with complete and accurate reports

Role of internal auditor

Internal auditor plays an important role in monitoring ERM, but do NOT have primary responsibility for its implementation or maintenance.

Support management by providing assurance on the

- ERM Process function
- Effectiveness and efficiency of risk responses and control activities.
- Completeness and accuracy of ERM reporting

Assist management and the board or audit committee in the process by:

- Monitoring
- Evaluating
- Examining
- Reporting
- Recommending improvements

Internal auditors can add value by:

- Reviewing critical control systems and risk management processes.
- Performing an effectiveness review of management's risk assessments and the internal controls.
- Providing advice in the design and improvement of control systems and risk mitigation strategies.
- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal auditing’s resources are directed at those areas most important to the organization.

- Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk treatment strategies.
- Facilitating ERM workshops.
- Defining risk tolerances where none have been identified, based on internal auditing's experience, judgment, and consultation with management.

Role of Business unit managers

They are responsible for operational risk.

- Establish operational context
- Identify operational risks
- Analyse operational risks
- Evaluate operational risks
- Treat operational risks
- Monitor and review operational risks
- Communicate and consult with the
- Leadership Team

Enterprise risks

Introduction

An event is any future activity that is going to have an impact on the business. An event can be a risk or an opportunity. While risk has a negative impact, an opportunity has a positive impact.

Risk can be defined as something that denotes a potential negative impact on something of value, a probability of incurring a loss. The scientific approach to risk entered finance in the 1980s when financial derivatives proliferated. Frank Knight has differentiated risk and uncertainty. He has restricted the term "uncertainty" to cases of the non-quantitative type.

The word "risk" comes from the same root as the Italian verb riscare, which means "to dare." In the quest for competitive advantage, businesses are nothing if not daring. Taking risks is essential. The more an organization can understand, predict and manage the dangers lurking in its path, the more it can turn daring behavior into the stuff of sustained success.

In Enterprise Risk Management, a risk is defined as a possible event or circumstance that can have negative influences on the Enterprise in question. Its impact can be either on the very existence; the resources (human and capital), the products and services, or the customers of the Enterprise, or it can be external impacts on Society, Markets or the Environment.

Misconceptions about risks

The three most common misconceptions about risks have now come to light. These are:

1. Risk only relates only to the down side – both negative and positive implications coexist and risk cannot be measured in the context of negative items only.
2. Risk depends only on the occurrence of an event – risk need not necessarily occur because of the occurrence of an event. Even the passage of time can cause risk.
3. Risk affects business only in the context of insurance – risk exists everywhere, at all levels.

Enterprise risk management is not just about buying insurance, it involves the identification, measurement, management and monitoring risks at all levels and for all processes in an enterprise as a continuous process.

Sources of risks

Risks could arise out of internal factors or external factors. External factors are:

- Macro economic factors
- Exchange rate fluctuations
- Political environment
- Competitive environment
- Business environment (cost, profit, regulations, competition, market fluctuations, etc.)
- Concentration of revenues
- Inflation and cost structure
- Immigration regulations
- Security and business continuity
- Product/service risks (configuration, technology, requirements, product/ service failure, etc.)
- Terrorism/sabotage
- Accidents
- Natural disasters
- General public opinion and reputation of the enterprise (trademark/brand erosion, fraud, unfavorable publicity)
- Customer wants
- Demographic and social/cultural trends
- Capital availability

Internal factors could be:

- Financial risk factors (risk from price - asset value, interest rate, foreign exchange, commodity; credit - default, downgrade; inflation/purchasing power; and hedging/ basis risk).
- Liquidity and leverage (cash flow, call risk, opportunity cost, etc.)
- Contractual compliance
- Compliance with local laws
- Intellectual property management
- Strikes/slowdowns
- Supply risks (exposure to compressed lead times, leaner inventories, dependence on single or few suppliers, more outsourcing, longer supply lines, etc.)
- More product introductions
- Integration, collaboration or acquisitions
- Human resource management (risk arising out of human error, skills, culture, values, leadership, change readiness, blind spots, etc.)
- Project risk factors (scope, schedule, resource availability, etc.)
- Operational risk factors (development and operational processes - capacity, efficiency, channel management, supply chain management, business cyclicality; information technology - relevance, availability; information/business reporting - budgeting and planning, accounting information, pension fund, investment evaluation, taxation)

When a business suffers physical damage as a result of a consequential loss like fire, flood, typhoon, storm surge, tsunami, etc, or a contingent loss due to supplier failure, customer, access, etc., the operation of the business might be interfered. This may cause the business to suffer a reduction in sales and/or incur additional costs. Such business interruptions are the largest losses that can cause a company to fail or can have the highest financial impact on the balance sheet if not properly addressed.

Banks or financial institutions face the following risks:

1. Market risk - When firm's value is affected by changes in Interest Rates, Exchange Rates, Stock Prices etc. It also includes liquidity risk.
2. Credit risk - Failure to meet the obligated payments of counter parties on time
3. Operational risk - failures in operating processes and systems, including security loss and fraud.
4. Legal and regulatory risks
5. Potential damage to business reputation

Other risks that could be faced by all enterprises are:

1. Inherent Risk - In the absence of any action, management might take to alter either the risk's likelihood or impact
2. Systematic Risk - The risk of holding Market Portfolio
3. Static Risk - Risk which is unique to an individual asset
4. Residual Risk - That remains after the action to mitigate risk is taken

Risks can also be classified as insurable or non insurable.

Generally, business interruptions and threats to assets and liabilities can be insured against.

Uninsured risks, if not managed properly, result in loss of revenue and increased costs. The reduced earnings lead to reduced dividend which in turn results in a fall in the share price. Uninsurable risks should be faced with policies like:

- Disaster Management Plan
- Business Continuity Plan
- Crisis Communication

Risks in an enterprise are interdependent and should be dealt with in an integrated manner for maximum value maximisation, hence the importance of enterprise risk management.

Industry Specific risks

Construction industry

Construction business is a complex and challenging process. Among other things, it requires interpretation of and conformance with a number of laws, codes and regulations, marshalling of considerable resources, including labor, equipment and material, and communication with and coordination among multiple parties, such as the design professional, contractor and subcontractors, all of whom may, at times, have different, even conflicting, purposes and goals. Moreover, many factors are unknown or unknowable at the start of any project. Hence risks are an inherent and expected part of this process.

The most serious effects of risks can be:

- failure to keep within the cost estimate
- Failure to complete within the stipulated time
- Failure to achieve the required quality and operational requirements

Every construction project is unique and each offers a multitude of different risks. To ensure the success of its undertaking, a company/corporate owner embarking on a construction project must be able to *recognize* and *assess* these risks.

Typical construction risks that may impact the project cost or schedule include the following:

1. Acts of God
    - Flood
    - Earthquake
    - Landslide
    - Fire
    - Wind damage
    - Lighting
2. Physical
    - Damage to structure
    - Damage to equipment
    - Labor injuries
    - Material and equipment fire and theft
3. Financial and economic
    - Inflation
    - Availability of funds with client
    - Exchange rate fluctuation
    - Financial default of sub-contactor
4. Political and environmental
    - Changes in laws and Regulations
    - War and social disorder
    - Requisitions for permits and their approvals
    - Pollution and safety rules
    - Customs and import restrictions and procedures
    - Insistence on use of local firms and agents
    - Encountering hazardous wastes, buried tanks, or other environmental conditions
    - Varying subsurface conditions encountering difficult soils, rock and groundwater

-

5. Design
    - Incomplete design
    - Defective design
    - Errors and omission
    - Inadequate specification
    - Different site conditions

6. Logistical Risks

- Availability of resources - particularly construction equipments, spares parts, fuel and labor.
- Availability of sufficient transportation facilities.

Risk response practices

There are four distinct ways of responding to risks in a construction project,

a) Risk Elimination

Risk elimination is sometimes referred to as risk avoidance. A contractor not placing a bid or the owner not proceeding with project funding are two examples of totally eliminating the risks. There are a number of ways through which risks can be avoided, e.g.

- tendering a very high bid;
- placing conditions on the bid;
- pre-contract negotiations as to which party takes certain risks; and
- not biding on the high risk portion of the contract

b) Risk Transfer

Risk transfer can take two basic forms:

(a) The property or activity responsible for the risk may be transferred, i.e. hire a subcontractor to work on a hazardous process; or

(b) The property or activity may be retained, but the financial risk transferred, i.e. by methods such as insurance

c) Risk Retention

There are two retention methods, *active* and *passive*. Active retention (sometimes referred to as self-insurance) is a deliberate management strategy after a conscious evaluation of the possible losses and costs of alternative ways of handling risks. Passive retention (sometimes called non-insurance), however, occurs through negligence, ignorance or absence of decision, e.g. a risk has not been identified and handling the consequences of that risk must be borne by the contractor performing the work.

d) Risk Reduction

Risk reduction is a technique within the overall risk management process, and is confined to the improvements of a company's physical, procedural, educational, and training devices.

- The physical devices can be improved by continually maintaining and updating the devices.
- Following of procedural aspects like housekeeping, maintenance, first aid procedures and security can lead to better morale, improved labor relations and increased productivity.
- Education and training within every department of a business are important, especially in reducing the harmful effects of risks within the

working environment. Loss prevention consumes capital resources, and with better education and training devices the effect may be minimized, freeing capital for more productive investments.

Pharmaceutical industry

The pharmaceutical industry is a high-tech industry with high value-added products. Generally pharmaceutical plants manufacture two different types of products, over-the-counter and prescription products

Pharmaceutical companies include:

- Pharmaceutical manufacturers
- Generic and OTC pharmaceutical companies
- Life sciences, biotechnology, and biopharmaceutical companies
- Genomic and proteomic companies
- Drug delivery system companies
- Diagnostic substance companies
- Medical device manufacturers

Risks could be involved in the following stages:

- manufacturing stage:
- product handling
- storage and
- packing

In the pharmaceuticals industry, various chemicals are being handled through several equipment, machinery and processes using electricity and mechanical devices. Various microorganisms are also being handled both in the laboratory

and in production process. So it is required to study the whole setup, machinery, process, raw materials, chemicals, microorganisms, etc. thoroughly. It is also required to identify all possible hazards and then take preventive and corrective measures to prevent the accident. In view of these, it is necessary to consider all these aspects for safety purpose during planning and implementation of project. This helps in prevention of accidents during running of plant.

Hazards in this industry include fire or explosion through solvents, flammable liquids or dusts and the resulting contamination of production and storage areas, particularly clean rooms by smoke or other substances released by the fire or equipment damage. Due to the medical nature of the products produced, companies may only be licensed to manufacture at specific production facilities. Re-certification of contaminated production lines can be a lengthy procedure and can lead to a loss of market share.

Specific risks that are a great threat to this industry include:

a) Product Liability

Pharmaceutical company regards product liability as its greatest threat. In addition to liability claims which can be covered by traditional risk transfer methods, companies are more concerned about the damage that a major loss could cause to their image. One of the unique problems in dealing with the product liability is the difficulty of building meaningful risk models. The severity and timing of future claims is highly unpredictable. As a result, the risk managers have to cope with the possibility that a major liability claim can threaten the solvency of their business without their ever knowing just how severe the claim might be.

Although pharmaceutical companies go to great lengths to limit their product liability risks by using quality assurance techniques and stringent pre – clinical

studies and extensive clinical tests that are legally required to be carried out, even the most sophisticated controls cannot entirely prevent the occurrences.

b) Business Interruption

The second most critical concern identified is the risk of a breakdown in the production process. The trend towards centralized production, either in a single unit, or with several units carrying out individual tasks, has increased this risk. A single stoppage could have far-reaching consequences.

The effect of business interruption is more complicated in the pharmaceutical industry. To begin with, those who depend on particular medication must continue to receive their supplies. If the pharmaceutical company has enough inventories to cover the production shortfall, this may not be problematic. Unfortunately, strict regulations governing the storage of drugs combined with their often short shelf-life make this a limited option. Moreover the storage facility itself may have been either lost or contaminated, especially where storage and production occupy nearby units.

The risk managers must also consider how to replace intermediate compounds used at different stages in the production process. The later in the chain the interruption occurs, the harder it is to remedy. To avoid a catastrophic loss, companies must have either the capacity to switch production elsewhere, or be able to produce compounds from other sources.

c) Patent Infringement

Protecting intellectual property is considered to be a critical risk for pharmaceutical companies. This reflects the fierce increasing competitive environment for both R&D and product offerings. The companies are generally more concerned about possible financial losses resulting from the infringement

of their own patents than about unintentional infringement of other company's patents.

Moreover, the growing number of counterfeit products hitting the market represents a considerable threat to the established companies, especially where the copy sports the company's brand name.

d) Product Recall

The risk involved is the subsequent damage to a pharmaceutical business public image. A product image is tarnished by the publicity the product attracts when it is removed from retail shelves. This is aggravated by its unavailability as consumers turn to alternative products. The fundamental goal of a re launch must be to restore public image

e) Research and Development

The pharmaceutical companies depend increasingly on Research and Development to stay competitive and to promote better earnings growth, especially as profit margins are under increased pressure and market competition has intensified. While events such as fire and natural perils might disrupt or completely destroy an R&D program, wrongly assessed experimental results or new findings in the later stages of product development could prove equally detrimental.

Some risk managers take risk in relation to political risk, foreseeing events – particularly in countries where patent piracy is an issue – that would limit access to essential materials and damage an R&D program.

f) Environmental Risk

Environmental risk plays a dominant role in the companies global risk assessment. The perception of environmental risk is consistent across all corporate types, regardless of whether they have large chemical or agrochemical units. This growing unease may be rooted in intensified environmental regulations and the host of new laws, or may be due to fears that new risks, such as those related to genetic engineering, will potentially impact the environment.

g) Other Risks

Among the multitude of other risks, two merit more detailed consideration: Political risk and financial risk. As far as political risk is concerned, the industry's attention is focused on protecting assets from nationalization, as well as on the potential disturbance of production and distribution. As pharmaceutical companies grow internationally and interdependencies develop, risk managers increasingly have to build global protection strategies that address the problems associated with political risk.

Chemical Industry

The chemical industrial sector is highly heterogeneous encompassing many sectors like organic, inorganic chemicals, dyestuffs, paints, pesticides, specialty chemicals, etc. Some of the prominent individual chemical industries are caustic soda, soda ash, carbon black, phenol, acetic acid, methanol and azo dyes

The risks associated with the chemical industry are commensurate with their rapid growth and development. Apart from their utility, chemicals have their own inherent properties and hazards. Some of the chemicals can be flammable, explosive, toxic or corrosive etc. The whole lifecycle of a chemical should be considered when assessing its dangers and benefits. Though many of chemical

accidents have a limited effect, occasionally there are disasters like the one in Bhopal, India, in 1984, where lakhs of people were affected and LPG explosion in Vizag refinery where huge property damage in addition to 60 deaths was experienced. Therefore chemicals have the potential to affect the nearby environment also.

The following points have to be borne in mind with regard to risks management:

a) Design and Pre-modification review : Improper layout like location of plant in down wind side of tank farm , fire station near process area , process area very close to public road and wrong material of selection can cause severe damages to the work and outside environment
b) Chemical Risk Assessment: new chemicals need to be assessed from the point of view of compatibility, storage, fire protection, toxicity, hazard index rating, fire and explosion hazards
c) Process Safety Management like Hazard & Operability (HAZOP) ,Failure Tree Analysis (FTA) ,reliability assessment of process equipment, incorporating safety trips and interlocks, scrubbing system, etc. need to be done before effecting major process changes,
d) Electrical Safety: Hazardous area classification, protection against static electricity, proper maintenance of specialized equipment like flameproof etc have to be taken care of.
e) Safety Audits: Periodical assessment of safety procedures and practices, performance of safety systems and gadgets along with follow up measures has to be carried out.
f) Emergency Planning: specific written down and practiced emergency procedures along with suitable facilities need to laid down.
g) Training: Safety induction and periodical refresher training for the regular employees and contract workmen have to be carried out.

Software Industry

Like all projects, software projects have risks. Risks that were not foreseen and planned for frequently cause major project issues and even failures. Such risks could be due to problems in the project or due to external events. For example things like changing requirements, integration problems, unavailability of skills, design issues; faulty technologies and so on are a frequent cause of problems. These sorts of issues are usually a challenge and a major source of worry for project supervisors, their managers and executive sponsors. Often their existence is recognized very late and desperate attempts are made to somehow mitigate their impact. However, recognizing them early and taking steps to address them can help bring the project back onto its tracks or in the worst case help make a decision to terminate the project before too much time and money is spent.

Common risks in software project management (as listed by Barry W. Boehm ,a pioneer in software risk management) include

- Personnel shortfalls
- Unrealistic schedules & budgets
- Developing the wrong functions & properties
- Developing the wrong user interface
- Continuing stream of requirements changes
- Shortfalls in externally furnished components
- Shortfalls in externally performed tasks
- Real-time performance shortfalls
- Straining computer-science capabilities
- Gold plating (features that duplicate what is already available)

Besides, the above, the following are several typical risk categories and risk items that may threaten any project. There are no magic solutions to any of these risk factors, so we need to rely on past experience and a strong knowledge of contemporary software engineering and management practices to control those risks

Dependencies

Many risks arise because of dependencies these project have on outside agencies or factors. As it is difficult to control these external dependencies, mitigation strategies may involve contingency plans to acquire a necessary component from a second source, or working with the source of the dependency to maintain good visibility into status and detect any looming problems. Here are some typical dependency-related risk factors:

- customer-furnished items or information
- internal and external subcontractor relationships
- inter-component or inter-group dependencies
- availability of trained, experienced people
- reuse from one project to the next

Requirements Issues

Many projects face uncertainty and turmoil around the product's requirements. While some of this uncertainty is tolerable in the early stages, the threat to success increases if such issues are not resolved as the project progresses. If requirements-related risk factors are not controlled either the wrong product may be built, or the right product may be built badly. Either situation results in unpleasant surprises and unhappy customers. Become familiar with established requirements gathering and management practices, and watch out for these risk factors:

- lack of clear product vision
- lack of agreement on product requirements
- requirements not prioritized
- new market with uncertain needs
- new applications with uncertain requirements
- rapidly changing requirements
- ineffective requirements change management process
- inadequate impact analysis of requirements changes

Management Issues

- inadequate planning and task identification
- inadequate visibility into actual project status
- unclear project ownership and decision making
- unrealistic commitments made, sometimes for the wrong reasons
- managers or customers with unrealistic expectations
- staff personality conflicts
- poor communication

Lack of Knowledge

The rapid rate of change of software technologies, and the increasing shortage of skilled staff, means that project teams may not have the skills needed to be successful. The key is to recognize the risk areas early enough so that we can take appropriate preventive actions, such as obtaining training, hiring consultants, and bringing the right people together on the project team. Inadequate training

- poor understanding of methods, tools, and techniques
- inadequate application domain experience
- new technologies or development methods
- ineffective, poorly documented, or neglected processes

Other Risk Categories

- unavailability of development or testing equipment and facilities
- inability to acquire resources with critical skills
- turnover of essential personnel
- unachievable performance requirements
- problems with language translations and product internationalization
- technical approaches that may not work

Banking Industry

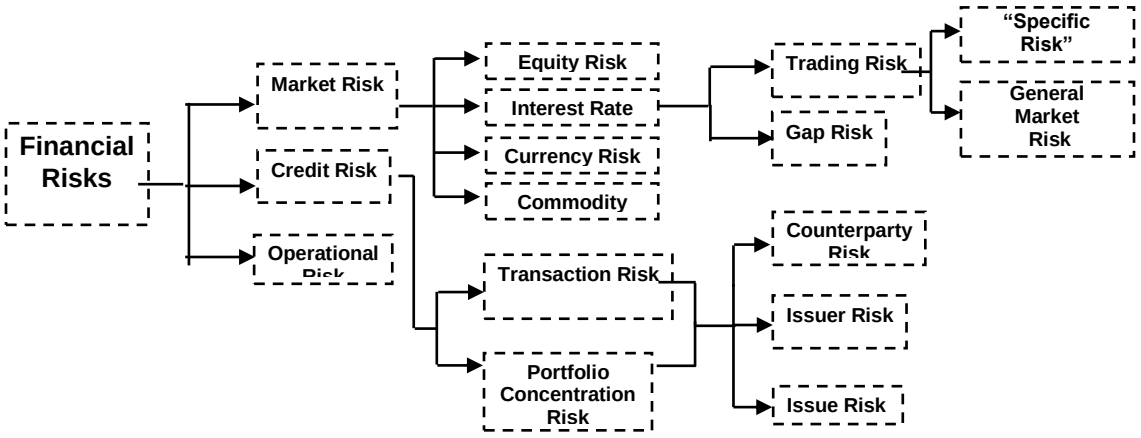
The risks in banking are a result of many diverse activities, executed from many locations, and by numerous people. The volatile nature of the bank's operating environment will aggravate the effect of these risks.

Types of financial risks:

Risks in banking companies can be clubbed under 3 categories

- Credit risk- this emanates owing to default in the counter party in respect of funded and non-funded exposures
- Market risk arising from change in market variable in the form of liquidity constraints, prices, exchange rates etc.
- Operational risk - is defined by BASEL II as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Although the risks apply to any organisation in business it is of particular relevance to the banking regime where regulators are responsible for establishing safeguards to protect

against systemic failure of the banking system and the economy. The Basel II definition includes legal risk, but excludes strategic risk: i.e. the risk of a loss arising from a poor strategic business decision. This definition also excludes reputational risk (damage to an organisation through loss of its reputation or standing) although it is understood that a significant but non-catastrophic operational loss could still affect its reputation possibly leading to a further collapse of its business and organisational failure.



The Prominent risks are explained below:

Market risk

Market risk is the financial risk of uncertainty in the future market value of a portfolio of assets and/or liabilities

Credit Risk

Credit risk or default risk involves inability or unwillingness of a customer or counterparty to meet commitments in relation to lending, trading, hedging, settlement and other financial transactions. The credit risk of a bank's portfolio depends on both external and internal factors.

The external factors are the state of the economy, wide swings in commodity/equity prices, foreign exchange rates and interest rates, trade restrictions, economic sanctions, Government policies, etc.

The internal factors are deficiencies in loan policies, administration, absence of prudential credit concentration limits, inadequately defined lending limits for Loan Officers/Credit Committees, deficiencies in appraisal of borrowers' financial position, excessive dependence on collaterals and inadequate risk pricing, absence of loan review mechanism and post sanction surveillance, etc.

Liquidity Risk

Liquidity risk is financial risk from a possible loss of liquidity. There are two types of liquidity risk:

- Specific liquidity risk is the risk that a particular institution will lose liquidity. This might happen if the institution's credit rating fell or something else happened which might cause counterparties to avoid trading with or lending to the institution.
- Systemic liquidity risk affects all participants in a market. It is the risk that an entire market will lose liquidity. Financial markets tend to lose liquidity during periods of crisis or high volatility.

Liquidity risk tends to compound other risks. It can be most damaging for institutions that are experiencing financial difficulties which create a need for immediate cash.

Operational Risk

Operational risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. This risk is associated with human error, system failures and inadequate procedures and controls.

Interest Rate Risk

Interest rate risk is the risk of an adverse effect of interest rate movements on a bank's profits or balance sheet. Interest rates affect a bank in two ways - by affecting the profits and by affecting the value of its assets or liabilities.

Foreign Exchange Risk

Foreign Exchange Risk is the chance that a fluctuation in the exchange rate will change the profitability of a transaction from its expected value. It is the risk that arises due to unanticipated changes in exchange rates,

Response to financial risks

- Market response-introduce new products
  - Equity futures
  - Foreign currency futures
  - Currency swaps
  - Options
- Regulatory response
  - Prudential norms
  - Stringent Provisioning norms

  - Corporate governance norms

Evolution of the regulatory environment

- G-3- recommendation in 1993
  - 20 best practice price risk management recommendations for dealers and end-users of derivatives
  - Four recommendations for legislators, regulators and supervisors
- 1988 BIS Accord [BASEL I]
  - 1996 amendment
- BASEL II

BASEL I accord provided for:

- Two minimum standards
  - Asset to capital multiple
  - Risk based capital ratio (Cooke ratio)
- Calculate risk weighted assets for on-balance sheet items
- Assets are classified into categories
- Risk-capital weights are given for each category of assets
- Asset value is multiplied by weights
- Off-balance sheet items are expressed as credit equivalents

BASEL II ACCORD

Basel II, also called The New Accord (correct full name is the *International Convergence of Capital Measurement and Capital Standards - A Revised Framework*) is the second Basel Accord and represents recommendations by bank supervisors and central bankers from 10 countries making up the Basel Committee on Banking Supervision to revise the international standards for measuring the adequacy of a bank's capital. It was created to promote greater consistency in the

way banks and banking regulators approach risk management across national borders.

Basel Committee proposed a 3 pillar approach as detailed under

Pillar 1: Minimum Capital Requirements: Under this, as in the current accord, a minimum capital has been prescribed to be maintained.

To arrive at the capital for various types of risks, a number of approaches, widely classified as standardised approach and internal approach, have been prescribed. The critical issues in the internal approach in which the banks are free to develop their own approach to measuring risks, are validating the internal approach and ensuring consistency across banks. The approaches for various types of risks are as under:

Credit risk

1. Standardized approach (External Ratings)

    - Provides Greater Risk Differentiation than 1988
    - Risk Weights based on external ratings
    - Five categories [0%, 20%, 50%, 100%, 150%]
    - Certain Reductions
    - e.g. short term bank obligations
    - Certain Increases
    - e.g.150% category for lowest rated obligors

The standardized approach is based on external credit assessment institutions

- Sovereigns

- Banks/securities firms
- Corporates
- Public sector entities
- Asset securitization programs

The risk weights w.e.f. January 2001 are:

Claim		Assessment					
		AAA to AA-	A+ to A-	BBB+ to BBB-	BB+ to BB-	Below BB-	Unrated
Sovereigns		0%	20%	50%	100%	150%	100%
Banks	Option 1[1]	20%	50%	100%	100%	150%	100%
	Option 2 [2]	20%	50% [3]	50% [3]	100% [3]	150%	50% [3]
Corporates		20%	50%	100%	100%	150%	100%

1. Risk weighting based on risk weighting of sovereign in which the bank is incorporated.
2. Risk weighting based on the assessment of the individual bank.
3. Claims on banks of a short original maturity, for example less than six months, would receive a weighting that is one category more favourable than the usual risk weight on the bank's claims

2. Internal ratings-based approach

This has a two tier ratings system: Obligor rating - represents probability of default by a borrower; and facility rating - represents expected loss of principal and/or interest

The three elements of the approach are:

- Risk Components
    - Probability of default ["conservative view of long run average (pooled) for borrowers assigned to a RR grade."] – what is the probability of counterparty defaulting?
    - Loss given default – if default occurs, how much do we expect to loose?
    - Exposure at default – if default occurs, how much exposure do we expect to have?
- Risk Weight conversion function
- Minimum requirements for the management of policy
- and processes
- Emphasis on full compliance

Risk components:

- Foundation approach - Probability of default set by Bank; Loss given default, Exposure at default set by Regulator - 50% Loss Given Default for Senior Unsecured will be reduced by collateral (Financial or Physical)
- Advanced approach - Probability of default, Loss given default, Exposure at default all set by Bank

3. Credit risk modeling (Sophisticated banks in the future)

The derivation of the default loss distribution in this model comprises the following steps

- Modeling the frequencies of default for the portfolio
- Modeling the severities in the case of default

- Linking these distributions together to obtain the default loss distribution

Credit risk mitigation involves recognition of wider range of mitigants and is subject to meeting minimum requirements. It applies to both Standardized and IRB Approaches. Credit risk mitigants are:

- Collateral
  - Simple approach (standardized only)
  - Comprehensive approach (coverage of residual risks through haircuts and weights)
- guarantees
- credit derivatives
- on balance sheet netting.

Market risk

A scenario analysis measures the change in market value that would result if market factors were changed from their current levels, in a particular specified way. No assumption about probability of changes is made.

Value at risk is a statistical measurement of risk. It is a single number that summarizes the likely loss in value of a portfolio over a given time horizon with specified probability. Three approaches are:

- Historical simulation
- Model-building approach
- Monte-Carlo simulation

Operational risk

Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems of external events. It excludes "Business Risk" and "Strategic Risk". It could be legal liability; regulatory/ compliance/taxation penalties; loss of or damage to assets; theft, fraud or unauthorized activities; transaction processing risk, etc.

The four increasingly risk sensitive approaches are:

1. Basic indicator - based on a single indicator
2. Standardized approach - divides banks' activities into a number of standardized industry business lines
3. Internal measurement approach
4. Loss distribution approach

Pillar 2: Supervisory Review Process: This puts responsibility on the bank supervisors to ensure that banks follow rigorous processes, measure their risk exposures correctly and maintain capital in accordance with risk exposure. The recent initiatives of the RBI in the introduction of Risk Based Supervision and Risk Based Internal Audit is in conformity with this pillar.

Pillar 3: Market Discipline: This aims to strengthen the safety and soundness of the banking system through better disclosure of risk exposures and capital maintained. This is expected to help the market participants to better assess the position of banks.

With a view to ensuring migration to Basel II in a non-disruptive manner, the Reserve Bank has adopted a consultative approach. A Steering Committee

comprising of senior officials from 14 banks (private, public and foreign) has been constituted where Indian Banks' Association is also represented.

Keeping in view the Reserve Bank's goal to have consistency and harmony with international standards it has been decided that at a minimum, *all banks in India will adopt Standardized Approach for credit risk and Basic Indicator Approach for operational risk with effect from March 31, 2007.*

Enterprise Risk Management technology

The need for professional risk managers and consultants to deliver low-cost, highly-valued risk management services to their customers in today's business world demands the use of technology to enhance their productivity and effectiveness.

While generally, it has been found that technology drives markets, the enterprise risk management discipline has evolved ahead of the technology needed to support it. Each enterprise is unique and has variable parameters.

The challenges of enterprise risk management can be met only with the right people and technology. While people are needed for expertise and process management, technology is required primarily for consistency, collaboration, and communication. Technology is expensive, especially if contracted on a consultation basis, and the right one need to be chosen. ERM calls for repetition in processes which can be delivered by technological solutions. As software providers rise to meet the needs of the enterprises, companies are expected to benefit greatly from ERM technology as a cost saving solution. Reduced expense and implementation time thus, drives a technology based approach towards ERM.

One of the great challenges for risk managers is to be "masters of all trades and jacks of none". This is now possible with knowledge and research available at our fingertips. The marker for being knowledgeable and well informed has been moved to new horizons with the advent of the World Wide Web. The computer has unlocked the ability to do complex business risk analysis which has never before been possible.

Enterprise Risk Management technology must manage the complexity for an ERM program.

1) Root Cause: A framework that gets to the cause of issues makes follow-up straight forward and logical.

2) Motivation: Performance Management functionality that makes it easy to help line managers achieve process improvements to reduce costs, bottlenecks, and unnecessary risk translates into their embracing risk management.

3) Process Driven: Selecting the most relevant key risk indicators for each core business process from thousands of possibilities.

4) Cross Functional Risk: Features to deliver a portfolio view with interactive dashboards to drill down or cut across silos to identify dependencies between risks.

5) Operational Controls: Go beyond financial controls to also quantify the effect of controls on business goal achievement while maintaining accountability throughout the process.

6) Risk Tolerance: Embedding risk management processes within the existing corporate culture from enterprise-wide board room strategy to tactical planning and analysis.

7) Maturity Model: Enable the risk management department itself to accelerate adoption of best practices, to set program objectives and measures and to manage ERM program activities.

From where to obtain the technology

For immediate needs, the professional services solution route has to be taken. Risk based approaches used in technology solutions have historically been delivered by the risk management information systems market. They have provided solutions primarily for purchasing insurance and managing claims. Many new tools, however, are being developed by traditional market leaders, keeping the enterprise risk management requirements in mind.

Providers in the insurance, risk consulting, and accounting and audit industries outside the core risk management information systems market are also working on custom ERM solutions for clients.

Many companies are also developing their in house technologies. A few consulting companies and large corporations have actually designed customized ERM processes and tools. But these require costly and involved consulting engagements to uncover the information required for the systems.

ERM oriented tools tend to address electronic environments or other specific risk management disciplines. Integrated ERM tools covering all processes of the enterprise and also all elements of ERM (identification, measurement, management and monitoring) are not easily available.

Many enterprises are moving purchasing ERM solutions from vendors or developing them in house. However, given the complexity and diversity of ERM, the overall risk management needs, the process will continue to evolve for some time till a comprehensive and integrated solution is developed.

The company that takes time to properly evaluate and deploy one of the emerging technology tools in conjunction with, rather than after, the initiation of its ERM program will be the company that saves time, money and the consequences of not meeting the regulatory requirements.

A comprehensive technological solution, addressing key ERM processes in an integrated fashion, will take evolution through time. Such a system would require a platform accessible by many people across the organization, be expandable as the organization matures and enable collaboration and integration. The system must provide a level of automation beyond data input and recording and be adaptive to systemized business rules. It must support the diverse roles of stakeholders with customizable access and views in order to be relevant for administrators, providers, auditors, and others.

The system must also provide ease of use; support for the multiple needs of the broader organization; automations and adaptation of processes; a level of transparency; and the ability to provide a benchmark.

Economics, while pushing technological innovation by the principle of supply and demand, will also push companies to adopt ERM by the principle of competition.

Checklist for Assessment of Enterprise Risk Management

1. Senior Management

Are senior management:

1.1 Taking key risk judgments and providing clear direction?

- Are they routinely in a position to be aware of the key risks and have systems in place to ensure that this is up to date?
- Do they have a good understanding of the key risks facing the organization and their likely implications?
- Are the risks that could result in key objectives or service delivery responsibilities not being met identified and the likelihood of them maturing regularly assessed?
- Are key risks prioritized for action and mitigation actions identified and monitored?

1.2 Setting the criteria/arrangements for the organization's appetite/tolerance for taking on risk?

- Are they setting the criteria for acceptable and/or unacceptable risk?
- Are they setting the criteria for reference for Board consideration?
- Are they establishing the criteria/arrangements for escalation of consideration of risks at various levels in the organization etc)?

1.3 Supporting innovation?

- Is well-managed risk taking encouraged to help seize opportunities and support effective innovation?
- Is there support and reward for innovation and seizing opportunities to better deliver the organizations aims and objectives?
- Is individual success rewarded and support given by management when things go wrong despite risks being well managed, i.e. avoiding a blame culture?

1.4 Ensuring clear accountability for managing risk?

- Are appropriate members of staff clearly assigned responsibilities for assessing, reporting and managing identified risk and are these responsibilities regularly reviewed?
- Do those responsible have the necessary authority and support to discharge their responsibilities effectively?
- Do managers understand and take responsibility for the management of risk in their area?
- Are matters actively reported through the management arrangements and to the audit/risk committee or Board as appropriate?

1.5 Driving implementation of improvements in risk management?

- Are they proactive in supporting and encouraging effective risk management?
- Are they proactive in supporting and driving a culture embracing well-managed risk taking?
- Are they proactive in supporting and driving the embedding of effective risk management in the organizations core activities (i.e. policy making, planning and delivery)?
- Are they ensuring effective management of risks to the public?
- Are they ensuring effective communication about risks and risk issues?
- Are they ensuring that managers and staff are equipped with necessary skills, guidance and other tools?

2. Risk Strategy and Policies

2.1 Risk Management Strategy

Is there a risk management strategy which:

- Is endorsed by the Head of the organization/ Board / Audit Committee / Risk Committee?
- Sets out the organization's attitudes to risk?
- Defines the structures for the management and ownership of risk and for the management of situations in which control failure leads to material realization of risks?
- Specifies the way in which risk issues are to be considered at each level of business planning and delivery ranging from the corporate process to operational action and the setting of individual staff's objectives?
- Includes risk as an opportunity (if it can be managed effectively) as well as a threat?
- Allows for peer review and the benchmarking of risks where appropriate?
- Specifies how new activities will be assessed for risk and incorporated into risk management structures?
- Ensures common understanding of terminology used in relation to risk issues?
- Defines the structures for monitoring, review and gaining assurance about the management of risk?
- Defines the criteria that will inform assessment of risk and the definition of specific risks as key?
- Defines the way in which the risk register(s) and risk evaluation criteria will be regularly reviewed?
- Is it easily available to all staff and reviewed at least annually to ensure it remains appropriate and current?
- Does if allow for balancing the portfolio of risk?
- Does it support effective innovation and encourage well-managed risk taking to generate improved delivery of aims and objectives?

- Does it encourage and promote the integration of risk management into established procedures and arrangements for departmental business, ie policy making, planning (e.g. business plans, delivery plans, spending plans etc), delivery etc and does this include effective management of risks to the public (information on .Principles of Managing Risks to the Public. can be found at: www.risk-support.gov.uk)?
- Does it include effective communication about risk with staff and all stakeholders, inside and outside the organization and including management of risks to the public?

2.2 Risk Management Policy

- Does a formal risk policy (policies) exist and is this documented, endorsed by the head of the organization, clearly communicated, readily available to all staff and subject to regular review?
- Were views from in-house stakeholders (e.g. employees, internal experts, auditors etc) taken into account?
- Is the risk management policy (policies) integrated with established policies for all activities (i.e. policy, planning, delivery etc)
- Are there clear statements that set out a proactive approach to innovation, and are staff encouraged to read them?
- Is there an explicit policy to encourage well-managed risk taking where it has good potential to realize sustainable improvements in service delivery and value for money, and is this policy actively communicated to all staff?
- Is a common definition of risks and how they should be managed, clearly communicated and adopted by all staff throughout the organization with detailed guidance for staff drawing up or implementing programmes, policies, plans etc?

- Is there a policy on balancing the portfolio of risk within the overall risk appetite/tolerance and does this include seizing opportunities as well as dealing with threats?

3. People

Are people equipped and supported by:

3.1 The Culture of the organization?

- Is there a general culture of risk management at all levels?
- Do managers and staff feel able to raise risk related issues?
- Do staffs have clear reporting chains and mechanisms to raise risk issues?
- Do managers and staff feel able to raise risk issues even where this may be seen as bad news?
- Are they encouraged and empowered to identify and take opportunities that will better deliver aims and objectives?
- Are they confident that their concerns/ideas will be heard and acted on?
- Do staffs feel empowered to take well-managed risks?
- Are staffs rewarded for taking well-managed risks?
- Are staffs confident that they will not be blamed for failure when risks have been well managed?
- Are staffs encouraged to challenge practices, to identify new ways of doing things and to be innovative?
- Do the monitoring and reporting systems generate an expectation that action will be taken on issues raised?
- Is risk management encouraged as part of the established way of planning and delivering the organizations business?

- Is risk management performance embedded in recruitment and performance appraisal?
- Is risk management incorporated into quality measures, e.g. Investors in people?

3.2 Arrangements for allocation of Responsibility?

- Do staffs have properly delegated clear and appropriate responsibility for managing risks and seizing opportunities?
- Is this reflected in their personal objectives and annual assessment?
- Are they clear when matters should be referred elsewhere (e.g. line management, audit committee, risk committee, board etc) for consideration?

3.3 Arrangements to ensure staff Awareness?

- Are staffs aware of the importance of handling risks well, of being innovative and identifying and seizing opportunities to improve outcome performance?
- Are staffs aware of the risk management strategy and policy (ies)?
- Are they aware of the key objectives, priorities and main risks facing the organization as a whole?
- Are staffs aware of the key objectives, priorities and main risks facing their part of the organization?

3.4 Provisions to ensure appropriate risk management knowledge, experience and skills?

- Are staffs adequately trained and experienced in risk management relative to the needs of the organization and the particular job being done?
- Do staffs receive appropriate guidance and training on the typical risks that the organization faces in relation to their role/job, and the action to take in managing these risks?
- Do staffs use guidance effectively?
- Do they have good access to advice and expertise?
- Does the personal performance review include assessment of relevant risk management skills and establish development objectives to fill any gaps?
- Are arrangements in place to ensure new staff receiving early assessment of their development needs and appropriate guidance, training etc to rapidly address these needs?
- Does skills transfer place take place when consultants or risk management professionals work within local teams?

4. Partnerships

Are there appropriate mechanisms for?

4.1 Identifying, assessing and managing risk in Partnerships:

- Are the risks associated with working with other organisations assessed and managed?
- Are there arrangements to ensure a common understanding of the risks and how they can be managed (eg a joint/shared risk register, sharing of risk register information, agreed risk assessments etc)?
- Are there arrangements for agreed standards for assessing risks?
- Has the risk terminology/language been agreed?

- Is there clarity about who is carrying which risks and what the requirements are for providing information?
- Are those responsible for managing the risks empowered to do so?
- Are arrangements scaled to match the risks, size/importance of the project etc?
- Are all those organizations, which are likely to have some influence over the success of a programme or service to the public identified?
- Are there arrangements to ensure, where possible, selection of the most appropriate partnership approach (e.g. .arms length', partnering, PFI etc)?
- Is consideration being given to the need for a consistent and common approach to managing risks that cut across organization boundaries, for example cross-departmental projects?
- Do organizations understand and have confidence in the risk management arrangements of all those involved in the joint working or who could influence the success of the programme?
- Are there incentives for partners to manage risks effectively (i.e. is the risk reward balance right for each partner)?
- Is there clear responsibility and accountability for risks where delivery of results is through partners, e.g. some risks (e.g. reputation) may remain even though responsibility for delivery is with a partner?

4.2 Monitoring and reviewing performance

- Is there reliable and regular information (e.g. Key issues, risks to be monitored, scale of risks, how they will be managed) to monitor the risk management performance of all those organizations involved?
- Is it clear who will provide what monitoring information and are rights of access sufficient to obtain the necessary information?

- Are there arrangements for joint review of risks and how differences of judgment and/or perception will be resolved?

4.3 Provision and testing of contingency arrangements?

- Are there adequate contingency arrangements (including prioritization of mitigation action) to minimize the adverse effects on public service delivery of one or more party failing to deliver?
- Have the contingency arrangements been tested?

4.4 Identifying and addressing the implications of risk transfer?

- Has the extent to which risks can be transferred to organizations both public and private best placed to manage them been considered and acted upon?
- Are staffs encouraged to take responsibility for risks when they are best placed to do so rather than transferring them to other organizations?
- Where risks are transferred to a partner organization are accountabilities clearly established and capacity maintained to manage and monitor performance and take early action in the event of difficulty?

5. Processes

5.1 Is Risk Management being fully embedded in the organization's business processes?

- Is risk management embedded in key processes, e.g.:
  - Policymaking

- Project and programme management
- Operational management
- Performance management
- Business planning
- Delivery planning
- Spending Review

- Are there well-established approaches for (i) identifying risk and (ii) assessing and reporting risks that are effectively communicated, followed and fully understood by relevant staff?
- Is risk management ongoing and integrated with other procedures so that staff accepts it as a standard requirement of good management and not a one-off or annual activity?
- Are arrangements in place to ensure risks to the public are well managed, including:

  - Ensuring openness and transparency;
  - Promoting wide involvement and engagement;
  - Taking steps to promote proportionate and consistent action;
  - Ensure clarity in the validity and use of all relevant evidence;
  - Ensure those best placed to manage the risk are given the responsibility for so doing?
  - Are arrangements in place to ensure sufficiently early and effective communication on risks and risk issues with staff, internal and external stakeholders

5.2 Do the processes support innovation and the identification and seizing of opportunities?

- Are arrangements in place to identify opportunities that might be available if risks are well managed, (e.g. reduced need for elaborate

systems of oversight and control of service delivery and hence greater cost effectiveness and efficiency)?

- When practicable is a monetary or other numerical value put on risk to emphasize to staff the potential loss or missed opportunity which could occur if risks are not well managed?

5.3 Do the procedures ensure risk management arrangements are effective and reflect good practice?

- Are arrangements in place, such as reviews by internal audit, consideration by audit and/or risk committee, involvement of non-executive Director(s), peer review, benchmarking with other organizations etc, to ensure that risk management approaches are effective, efficient and reflect good practice?
- Are the arrangements for monitoring and review subject to review to ensure they remain appropriate, proportionate and cost-effective?
- Has management sought advice from internal and external audit on good practice in the development, implementation and maintenance of robust risk management processes and systems?
- Has professional advice been taken to ensure that the most appropriate tools and techniques are used to assess risk and the likelihood of it maturing?
- Are both internal and external experiences used to inform risk management processes and procedures?

5.4 Do the processes ensure appropriate resilience?

- Does the organization have a well-developed business/service continuity plan?
- Does the organization have an IT recovery plan?

- Is the action (i.e. contingency plans, business continuity plans) planned to deal with consequences of risks maturing (such as the impact on the delivery of services to the public) regularly reviewed (tested asappropriate) to ensure that it remains appropriate, sufficient and cost effective?

5.5. Risk identification and evaluation

Is there documentation which:

- Records identified risks and opportunities in a structured way to:
  - Record dependencies between risks?
  - Record linkages between lower level risks and higher-level risks?
  - identify key risks?
  - facilitate assignment of ownership at a level that has authority to assign resources to the management of the relevant risk?
- Evaluates risks using defined criteria that are applied consistently?
- Provides evaluation of inherent risk (before any control implemented) and residual risk (risk remaining after planned controls are implemented)?
- Evaluates risk-taking account of both:
  - The likelihood of the realization of the risk, and
  - The impact of the realization of the risk?
- Identifies assigned ownership of the risk?
- Records, in as far as it can be defined:

- The acceptable level of exposure in relation to each risk?

- Why it is considered that the defined acceptable level of exposure can be justified?

- Is a risk assessment carried out before commencing major projects and reviewed at intervals to determine its continued validity and identify any new and emerging risks?
- Is use made of feedback from the public (e.g. citizens. forum) to identify the public's perception and attitude to risk(s) and to help with identification of any unforeseen risks?
- Are early warning indicators in place covering for example, quality of service or seasonal increase in customer demand not being met to alert senior management of potential problems in service delivery or that the risk of planned outcomes not being met is increasing?
- Is horizon scanning used to spot emerging threats and opportunities?

5.6. Criteria for evaluation of risk

- Do specific criteria for evaluating risk encompass a range of factors, including:
  - Financial / value-for-money issues?
  - Service delivery / quality of service issues?
  - Public concern/public trust /confidence issues?
  - Degree and nature of risks to the public?
  - Reversibility or otherwise of realization of the risk?
  - The quality or reliability of evidence surrounding the risk?
  - The impact of the risk on the organization (including its reputation) / stakeholders (including the public) / partners / others?

- Defensibility of realization of the risk?

- Are these criteria applied consistently and methodically across the whole range of risks?

5.7 Risk control mechanisms

- Are controls in place in relation to each risk which is?
  - Based on active consideration of the options for controlling that risk to an acceptable level of residual exposure?
  - Promulgated to all those who need to know about the controls?
  - Regularly reviewed to consider whether they continue to be effective?
  - The best value for money response to the risk?
  - Documented by the relevant managers?
- In respect of key risks, including those which lie outside the control of the organization, are plans developed and documented contingent against the risk being materially realized despite the controls that are in place (i.e. to address the residual risk after control action)?
- Are there adequate Business Continuity arrangements?
- Are reliable contingency arrangements in place so that if problems arise services to the public will be maintained and the adverse impact on key programme outcomes such as late delivery or reduced qualitywill be minimised?

5.8 Arrangements for appropriate Communications

- Are there adequate means of communicating with staff about risk issues?
- Is there adequate communication with external stakeholders?

- Is there a reliable communications strategy in place so that if risks mature those most affected by the potential adverse consequences fully understand and have confidence in the remedial action that the organisation may need to take?
- Are communication issues considered at a sufficiently early stage to ensure implications can fully inform policy, programme etc development and implementation?

5.9. Review and assurance mechanisms

- Are review and assurance mechanisms in place to ensure that each level of management, including the Board, regularly reviews the risks and controls for which it is responsible?
- Are these reviews monitored by / reported to the next level of management?
- Is any need to change priorities or controls clearly recorded and either acted upon or reported to those with authority to take action?
- Are risk identification, assessment and control lessons that can be learned from both successes and failures identified and promulgated to those who can gain from them?
- Is an appropriate level of independent assurance provided on the whole process of risk identification, evaluation and control?
- Is the methodology for gaining independent assurance defined with particular reference to the role of internal audit and the audit committee (or assurance, risk committee etc), and to the role of non executive directors and any other review bodies working within the organization?
- Has any system of peer review and/or benchmarking been used to provide independent assurance of the approach used and the results?

7. Risk Management Action

Has risk management action contributed to:

- Effective anticipation and management of strategic risks?
- Effective decision and policymaking?
- Effective handling of cross cutting issues?
- Effective review and assurance?
- Effective planning and target setting?
- Effective risk allocation?
- Encouraging greater efficiency?
- Effective cash management?

The contents of a good Enterprise Risk Management framework

An Enterprise Risk Management Framework provides guidance to adopt a more holistic approach to managing risk. The application of the Framework is expected to provide employees and organizations a better understanding of the nature of risk, and to manage it more systematically.

The objectives of an ERM framework are:

- The management determine the level of risks acceptable to the enterprise;
- Strategic and operational risks arising from enterprise activities are identified and prioritised;
- Acceptable mitigation or treatment strategies to manage, transfer or avoid risks are in place;

- Risks and mitigation strategies are subject to review at regular intervals to determine that the nature of identified risks has not changed, evaluate new risks and ensure mitigation strategies remain acceptable and operational; and
- The board and its sub-committees, and senior management, receive periodic reports of the risk management process

Risk/return considerations should be incorporated in product development and pricing, relationship management, investment and portfolio management, and mergers and acquisitions to enable making of better decisions. Risk management is not just about protecting but can also be an important tool for improving business performance.

The features of an efficient ERM framework are discussed as under:

1. Easy to use and understand

The discipline required to implement an ERM program will never be viewed negatively if the system is simple to use and to incorporate in the regular routine. However, if the ERM framework is counter intuitive and difficult to learn, the employees would not easily adapt it; and even if they adapt, it would be difficult for them to follow it properly. Risk management issues should be clearly understood at all levels. Employees should understand how a risk based approach helps them achieve their goals. Accountability towards goals and risk's implications should be laid in such manner that it is easily understood by employees at all levels.

2. Documentation

A properly documented ERM framework is necessary not only for meeting the regulatory requirements or facilitating audit, but also for its smooth and effective

operation. The goals should also be properly documented and understood by all employees. There should be clear classification of risk and performance indicators. The risk culture for the enterprise should be laid down and understood by all; and the tolerable level of risk (risk appetite) should be specified for each aspect of risk. The risk assessment methodology, standard risk management context (strategic goals, business functions and processes, resources) and set of risk evaluation criteria (rare, unlikely, moderate, likely, almost certain, or any similar criteria) should be developed and updated from time to time.

3. Cover all segments of the enterprise

The ERM framework should support for the multiple needs of the broader organization and should be embedded with all the functions areas. It should provide for risk assessments to be consistently conducted in all business areas. Employees at all levels should use a risk based approach to achieve goals. The ERM framework should inculcate a risk culture such that risk management is clearly defined and practiced at every level. Both the upward and downward side of risks should be aggressively managed.

4. Standardization coupled with flexibility

The ERM system should have a certain degree of standardization and systemization for enterprise collaboration, but flexibility for the function or user specific application. Standardized evaluation criteria of impact, likelihood and ERM effectiveness should be used to prioritize risk for follow ups. Policy should be laid down to guide decision-making and attack gaps between perceived and actual risk.

5. Automation and adaptation of processes

The nature of ERM demands a repeatable process. An effective ERM framework will automate the repetitive processes and take much of the human risk out of the process. The system can alert and remind participants about an activity, a due date or a report. This will help ensure that nothing is overlooked making the process more efficient as the employees can focus on more added value work.

6. Transparency

The level of transparency a system can support is crucial – particularly when it comes to regulatory requirements. Technology can help in this. A system can capture and record an activity at a very low level. This can provide a clear and objective visibility to processes and controls without the need for outside consultants or auditors.

7. Meet the varying needs of all

Various departments have different needs. A system will actually help drive adoption and accountability if it can meet at least the majority of the needs of departments such as finance, human resources, regulatory, and information technology.

8. Meet regulatory and other requirements

The system should meet the standards and the regulatory requirements.

9. Audit trail

A clear, compatible and quantifiable audit trail is essential to an ERM program. The closer and more visibly a system can mirror an audit process or provide detailed reporting required to satisfy an audit, the better.

10. Ability to provide a benchmark

Because of the unique nature of each enterprise, it is difficult to have a set standard or guidance for an ERM framework. Hence, the only measurable standard available for an enterprise is itself. Self comparison should be made possible by an ERM system to compare the past, present and the future position of an enterprise.

11. Integrated into the planning process

An ERM framework should balance short term goals with the long term goals. Risk management should be an inherent part of goal setting. Sustainability aspects should be integrated into operational planning. Strategic opportunities should be routinely identified and evaluated as the risk plans develop. Deviations from plans or expectations should be continuously measured against goals. There should be resiliency (ability to spring back from and successfully adapt to adversity) planning for all components. Response procedures should be well documented. Process owners should be required to consistently manage their risks and opportunities within regular planning cycles. A long term business view should be promoted by the ERM framework.

12. Fixing responsibility and accountability

An efficient ERM framework has risk management accountability woven into all processes, support functions, business lines and geographies to achieve goals with process owners and risk ownership clearly defined. It has well defined risk management processes and specific risks identified.

13. Communication and reporting

The ERM framework should provide for frequented and effective communication of risk issues so that they can be acted upon in time. There should be clear reporting lines in the ERM framework so that line managers can

report their risk priorities to the senior management. Periodic reports should measure ERM progress at all levels. The effect of external and internal events effect on each project should be reported.

14. Part of operations

The ERM framework should require all operational managers to always effectively participate in the risk management process.

15. Human resource management

Risk management should be made a part of every performance review and promise makers held accountable. Effective risk management should be compensated and be part of career development. The ethics and trust should be shared among all employees so that they can work in coordination and understand the risk interdependencies.

16. Coordination

The ERM framework should promote integration, communication and coordination of internal audit, information technology, compliance, control and risk management. Everybody should understand the interdependencies of risk – risk in one department/geographical area has a ripple effect in the enterprise as a whole.

17. Risk assessments

The ERM framework should call for qualitative risk assessments for every project, new products, business practice changes and acquisitions and measure the effectiveness of managing uncertainties and seizing risk opportunities. Such analysis should act as a guide for further quantitative analysis. Risk assessments should determine the need for business continuity plans and analysis. The ERM

framework should provide for aggregation and analysis of risk assessment information and address dependencies. Differences between defined risk tolerance and actual risk should be regularly assessed.

18. Continuous process

The ERM framework should lay down the process for regular and continuous review of risk plans; consistent identification, measurement, management and monitoring of risks and their root causes in all business areas; and regular review of risk and performance assumptions. The root cause approach ensures that the problem and not the symptom is addressed. The effectiveness of the framework should be regularly monitored and assessed so that suitable action may be taken in time.

19. Technology

The technology should be in conjunction with the ERM program.

20. Cost benefit

The ERM framework should be established after an analysis of the costs and benefits. Resources should be allocated on the basis of reward priorities.

Regulatory environment and standards/best practices pertaining to enterprise risk management

Indian scenario

Clause 49 intends to protect the interest of the stakeholders through good corporate governance practices and disclosures. The revised Clause 49 has been made effective from January 1, 2006.

It requires reporting by the board of directors in "Management Discussion and Analysis" an appropriate disclosure on risk management, and for this the company is expected to lay down process to inform board members about the risk assessment and minimisation procedures. These procedures should be periodically reviewed to ensure that management controls risk through means of a periodically defined framework.

Risk management, therefore, is a critical component of corporate governance and an area of disclosure in the report of board of directors. However, most Indian companies view risk management to minimise the losses rather than looking as a comprehensive approach for maximising shareholder wealth.

One of the greatest and most important challenges for CEO and CFO is to define the optimal risk level for their business to ensure that the activities of the organisation produce risk-adjusted returns.

Boards must ensure that all significant risks are managed through a well-defined framework. The organisations are reasonably aware of the risks related to their specific business areas.

However, the measurement, consolidation and aggregation of risk exposure are rarely carried out in a systematic manner. Even when organisations are good at identifying various risks they face, they often make mistake in dealing with these risks in a piecemeal manner or they do not consider all options available to deal with the risks. The process requires substantial efforts, in identifying all the risks applicable to the company, then from within these to prioritise based on their potential impact and significance, and finally to identify holders for these key risks and to put in place mitigation plans considering all possible options.

An enterprise -wide view of risk management can greatly improve efficiencies and generate synergies.

Applicability of Clause 49

The provisions of the revised Clause 49 shall be applicable as follows:

- All listed entities having a paid up share capital of Rs 3 crores and above or net worth of Rs 25 crores or more at any time in the history of the company
- For other listed entities which are not companies, but body corporate (e.g. private and public sector banks, financial institutions, insurance companies etc.) incorporated under other statutes, the revised Clause 49 will apply to the extent that it does not violate their respective statutes and guidelines or directives issued by the relevant regulatory authorities.
- The revised Clause 49 is not applicable to Mutual Funds

Requirement under Clause 49 of the Listing Agreement with regard to Risk Management

Clause 49 (IV) (C) - Board Disclosures – Risk management

The company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

Clause 49 (IV) (D)- As part of the directors' report or as an addition thereto, a Management Discussion and Analysis report should form part of the Annual Report to the shareholders.

i. Industry structure and developments.

ii. Opportunities and Threats.

iii. Segment–wise or product-wise performance.

iv. Outlook

v. Risks and concerns.

vi. Internal control systems and their adequacy.

vii. Discussion on financial performance with respect to operational performance.

viii. Material developments in Human Resources / Industrial Relations front, including number of people employed.

Disclosures being made by Indian companies

The genesis of disclosure about risk management in the report under corporate governance is that transparent communication to investors about enterprise-wide risk management approach should create positive impact ultimately for creation of shareholder value.

In spite of making it mandatory for all listed companies in India to disclose (in their report of board of directors) the risks faced and the adequacy of risk-management processes in their organisation, the quality of such disclosures has not been satisfactory. Except for some of the leading software development companies, not many Indian companies have recognised the importance of integrated risk management.

Most of the companies are adopting defensive approach to minimise the negative impact of risks.

Hero Honda Ltd., a leading auto sector company, in its report has mention of slow down, competition and input costs as its risks. This is more like a general statement about the risks to theoretically comply with the reporting requirement.

Similarly, ACC Ltd., a leading cement manufacturing company, has just touched upon the availability of coal and transport bottlenecks as the likely risk factors to the company. The company is looking towards the Government for necessary steps to improve the situation.

NTPC Ltd., yet another leading public sector company, has reported some of the risks it is exposed to and is relying upon the systems and practices put in place since its inception for identification and mitigation of risks. Wipro Ltd. in its latest annual report has dealt with various types of risks in great details covering macroeconomic, geo-political, social and international developments such as taxation and foreign investment policies, regional conflicts in South Asia, political instability, unauthorised use of intellectual property rights, presence in market segments, cost management, competitive forces, immigration policy, technology adaptation, telecommunication disruptions etc. However, sensitivity analysis is absent.

Risk management in banks and financial institutions

Even in banks and financial institutions, where success largely depends on striking a balance between enhancing profits and managing risk, the attention to risk identification, measurement and monitoring is not adequate. This is evident from the quality of their risk reporting and disclosures. Mathematical modelling

and sensitivity analysis which indicate how much the company will be affected by risk exposure is missing in the disclosures. State Bank of India, the largest public sector bank of the country, in its report covers some of the risks it is exposed to and looks for dealing with them through internal control, audits and adhering to RBI guidelines.

The following guidelines have been issued by the Reserve Bank of India to serve as a benchmark to the banks, which are yet to establish integrated risk management systems:

1. Asset-Liability Management (ALM) guidelines issued vide circular DBOD.BP.BC.8/21.04.098/98-99 dated February 10, 1999
2. guidelines on Risk Management Systems were issued vide circular DBOD.No.BP.(SC).BC.98/ 21.04.103/99 dated October 7, 1999 covering broad contours for management of credit, liquidity, interest rate, foreign exchange and operational risks.

As a step towards enhancing and fine-tuning the existing risk management practices in banks, draft Guidance Notes on Credit Risk Management and Market Risk Management were issued to banks vide letters DBOD.BP.BC.26/21.04.103/2001 dated September 20, 2001 and DBOD.BP.1913/21.04.103/2001 dated March 26, 2002, respectively.

The Guidance Notes were based on the recommendations of two Working Groups constituted in Reserve Bank of India drawing experts from select banks and Financial Institutions.

Comments on these Guidance Notes were received from a wide spectrum of banks, financial and academic institutions, rating agencies and other market participants.

The draft Guidance Notes on Management of Credit Risk and Market risk have been revised in the light of the feedback received and the revised Guidance Notes are now placed on the website of RBI (http://www.rbi.org.in). [DBOD. No. BP. 520 /21.04.103/2002-03 October 12, 2002]

Banks may use these Guidance Notes for upgrading their risk management systems.

The design of risk management framework should be oriented towards the banks' own requirements dictated by the size and complexity of business, risk philosophy, market perception and the expected level of capital. The systems, procedures and tools prescribed in the Guidance Notes for effective Management of Credit Risk and

Market Risk may, therefore, be treated as indicative. The risk management systems in banks should, however, be adaptable to changes in business size, the market dynamics and the introduction of innovative products by banks in future.

The bank is now looking for designing, monitoring and implementing an appropriate structure for integrated risk management. Many of the banks have constituted Asset Liability Management Committee (ALCO) to evolve optimal asset/liability structure on ongoing basis and Operations Risk Management Committee (ORMC) to oversee operational risks and the requisite control measures. However, the banks do not seem to have quantified risk impact.

The future of enterprise risk management

With globalisation of markets, the importance of non-traditional risks arising from customer loyalty, competition, operational hazards and acquisition & mergers are increasing. More frequent changes in interest rates and growing recognition of the Indian Rupee in international trade is making exchange rate more volatile than before. Moreover, pressure for compliance from legal and regulatory authorities, better corporate governance practices, growing tendency for greater transparency in reporting and increasing investor awareness will see companies in India look at enterprise risk management as a proactive approach to add value for their stakeholders. CFOs will have a bigger role to play in this direction.

International scenario

Risk assessment and Corporate governance rules – NYSE

Corporate governance rules of the New York Stock Exchange approved by the SEC on November 4, 2003, other than Section 303A.08, which was filed separately and approved by the SEC on June 30, 2003:

The duties and responsibilities of the audit committee – which, at a minimum, must include those set out in Rule 10A-3(b)(2), (3), (4) and (5) of the Exchange Act , as well as to:

(D) discuss policies with respect to risk assessment and risk management;

While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee

must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee.

(d)

Each listed company must have an internal audit function.

Listed companies must maintain an internal audit function to provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control. A company may choose to outsource this function to a third party service provider other than its independent auditor.

Risk Assessment and Sarbanes Oxely Act

Section 404 of the Sarbanes-Oxley Act of 2002 required U.S. publicly-traded corporations to utilize a control framework in their internal control assessments. Many opted for the COSO Internal Control Framework, which includes a risk assessment element. The term top down risk assessment (TDRA) is used by the PCAOB and the Securities Exchange Commission (SEC).

Detailed guidance about performing the TDRA is included with PCAOB Auditing Standard No. 5 and the SEC's interpretive guidance (Release 33-8810/34-55929) "Management's Report on Internal Control over Financial Reporting"). This guidance is applicable for 2007 assessments for companies with 12/31 fiscal year-ends. The PCAOB release superseded the existing PCAOB

Auditing Standard No. 2, while the SEC guidance is the first detailed guidance for management specifically.

TDRA is a hierarchical framework that involves applying specific risk factors to determine the scope and evidence required in the assessment of internal control. Both the PCAOB and SEC guidance contain similar frameworks. At each step, qualitative or quantitative risk factors are used to focus the scope of the SOX404 assessment effort and determine the evidence required. Key steps include:

1. identifying significant financial reporting elements (accounts or disclosures)
2. identifying material financial statement risks within these accounts or disclosures
3. determining which entity-level controls would address these risks with sufficient precision
4. determining which transaction-level controls would address these risks in the absence of precise entity-level controls
5. determining the nature, extent, and timing of evidence gathered to complete the assessment of in-scope controls

Management is required to document how it has interpreted and applied its TDRA to arrive at the scope of controls tested. In addition, the sufficiency of evidence required (i.e., the timing, nature, and extent of control testing) is based upon management (and the auditor's) TDRA. As such, TDRA has significant compliance cost implications for SOX404.

Frequent interaction between management and the external auditor is essential to determining which efficiency strategies for SOX assessment will be effective in each company's particular circumstances and the extent to which control scope reduction is appropriate.

Risk assessment and PCAOB Auditing Standards

The relevant Standards issued by the US Public Company Oversight Board (PCAOB) are discussed as under:

Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements

This standard establishes requirements and provides directions that apply when an auditor is engaged to audit both a company's financial statements and management's assessment of the effectiveness of internal control over financial reporting.

24. The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements.

Company's risk assessment processes is a part of such controls.

39. When planning the audit of internal control over financial reporting, the auditor should evaluate how the following matters will affect the auditor's procedures:

… Preliminary judgments about materiality, risk, and other factors relating to the determination of material weaknesses.

49. The auditor must obtain an understanding of the design of controls related to each component of internal control over financial reporting, as discussed below.

- *Control Environment.*

- *Risk Assessment - When obtaining an understanding of the company's risk assessment process, the auditor should evaluate whether management has identified the risks of material misstatement in the significant accounts and disclosures and related assertions of the financial statements and has implemented controls to prevent or detect errors or fraud that could result in material misstatements. For example, the risk assessment process should address how management considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.*
- *Control Activities.*
- *Information and Communication.*
- *Monitoring*

52. Identifying Company-Level Controls. Controls that exist at the company-level often have a pervasive impact on controls at the process, transaction, or application level. For that reason, as a practical consideration, it may be appropriate for the auditor to test and evaluate the design effectiveness of company-level controls first, because the results of that work might affect the way the auditor evaluates the other aspects of internal control over financial reporting.

- *…*
- *Management's risk assessment process;*
- *Board-approved policies that address significant business control and risk management practices.*

72. Different types of major classes of transactions have different levels of inherent risk associated with them and require different levels of management supervision and involvement. For this reason, the auditor might further categorize the identified major classes of transactions by transaction type: routine, nonroutine, and estimation.

Auditing Standard No. 4 – Reporting On Whether a Previously Reported Material Weakness Continues To Exist

This standard establishes requirements and provides direction that apply when an auditor is engaged to report on whether a previously reported material weakness in internal control over financial reporting (hereinafter referred to as a material weakness) continues to exist as of a date specified by management.

Auditing Standard 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements [Released on 12th June 2007]

This standard establishes requirements and provides direction that applies when an auditor is engaged to perform an audit of management's assessment1/ of the effectiveness of internal control over financial reporting ("the audit of internal control over financial reporting") that is integrated with an audit of the financial statements.

10. Risk assessment underlies the entire audit process described by this standard, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control.

11. A direct relationship exists between the degree of risk that a material weakness could exist in a particular area of the company's internal control over financial reporting and the amount of audit attention that should be devoted to that area. In addition, the risk that a company's internal control over financial reporting will fail to prevent or detect misstatement caused by fraud usually is higher than the risk of failure to prevent or

detect error. The auditor should focus more of his or her attention on the areas of highest risk. On the other hand, it is not necessary to test controls that, even if deficient, would not present a reasonable possibility of material misstatement to the financial statements.

12. The complexity of the organization, business unit, or process, will play an important role in the auditor's risk assessment and the determination of the necessary procedures.

Addressing the Risk of Fraud

14. When planning and performing the audit of internal control over financial reporting, the auditor should take into account the results of his or her fraud risk assessment. As part of identifying and testing entity-level controls, as discussed beginning at paragraph 22, and selecting other controls to test, as discussed beginning at paragraph 39, the auditor should evaluate whether the company's controls sufficiently address identified risks of material misstatement due to fraud and controls intended to address the risk of management override of other controls. Controls that might address these risks include –

• Controls over significant, unusual transactions, particularly those that result in late or unusual journal entries;

• Controls over journal entries and adjustments made in the period-end financial reporting process;

• Controls over related party transactions;

• Controls related to significant management estimates; and

• Controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results.

15. If the auditor identifies deficiencies in controls designed to prevent or detect fraud during the audit of internal control over financial reporting, the auditor should take into account those deficiencies when developing his or her response to risks of material

misstatement during the financial statement audit, as provided in AU sec. 316.44 and .45.

Using a Top-Down Approach

21. The auditor should use a top-down approach to the audit of internal control over financial reporting to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to internal control over financial reporting. The auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions.

This approach directs the auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the ***financial statements and related disclosures****. The auditor then verifies his or her understanding of the risks in the company's processes and selects for testing those controls that sufficiently address the assessed risk of misstatement to each relevant assertion.*

The top-down approach describes the auditor's sequential thought process in identifying risks and the controls to test, not necessarily the order in which the auditor will perform the auditing procedures.

Identifying Entity-Level Controls

22. The auditor must test those entity-level controls that are important to the auditor's conclusion about whether the company has effective internal control over financial reporting. The auditor's evaluation of entity-level controls can result in increasing or decreasing the testing that the auditor otherwise would have performed on other controls.

24. Entity-level controls include –

… The company's risk assessment process;

Policies that address significant business control and risk management practices.

New guidance issued by the Securities and Exchange Commission (SEC) and PCAOB in 2007 placed increasing scrutiny on top-down risk assessment and included a specific requirement to perform a fraud risk assessment. Fraud risk assessments typically involve identifying scenarios of potential (or experienced) fraud, related exposure to the organization, related controls, and any action taken as a result.

Regulation Asset Backed Securities [United States]

The structure of assetbacked securities is intended, among other things, to insulate ABS investors from the corporate credit risk of the sponsor that originated or acquired the financial assets.

The registration, disclosure, and reporting requirements for publicly issued asset-backed securities (ABS) are governed by the Securities Act of 1933 and the Exchange Act of 1934. The modern asset-backed securitization market did not exist at the time of the creation of these laws, and as a result, the process of asset-backed security registration has been revised several times by Congress and the Securities and Exchange Commission (SEC) to better reflect the needs of the ABS market.

On December 24, 2004, the Securities Exchange Commission approved the final form of Regulation AB, which provides a comprehensive set of federal securities rules and regulations for asset-backed securities.

On January 7, 2005, the SEC published Regulation AB, a final rule to codify requirements for the registration, disclosure and reporting for all publicly registered asset-backed securities including mortgage-backed securities.

Regulation Asset Backed Securities, popularly called Regulation AB:

- Updates and clarifies the Securities Act registration requirements for ABS offerings
- Provides disclosure guidance and requirements for Securities Act and Exchange Act filings involving ABS
- Establishes a consistent servicing standard that is used as the basis for measuring
- Requires an accountant's attestation report for each service assertion

Health Insurance Portability and Accountability Act [HIPAA]

The Health Insurance Portability and Accountability Act of 1996 requires the implementation of progressive controls in the handling of patient information. This covers not only control of the data itself and of electronic security, but also control over who has access to the information, as well as implementation of training and education of those handling the information and processes to eliminate breaches.

Section 164.308(a)(1) of HIPAA requires an organization to conduct the risk analysis of the organization. This analysis is required to understand the flow of e-PHI in the organization and the result of this analysis will facilitate creation of security policies & procedures and support the recommendation to initiate the HIPAA Security Compliance related remediation activities.

Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable

precautions necessary to prevent PHI from being used for non-health purposes.) This is an auditable on going process.

OMB Circular No. A-123

Office of Management and Budget, United States' Circular No. A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. Management controls guarantee neither the success of agency programs, nor the absence of waste, fraud, and mismanagement, but they are a means of managing the risk associated with Federal programs and operations. To help ensure that controls are appropriate and cost-effective, agencies should consider the extent and cost of controls relative to the importance and risk associated with a given program.

Federal Deposit Insurance Corporation Improvement Act of 1991 [FDICIA] [United States]

The act mandated a least-cost resolution method and prompt resolution approach to problem and failing banks and ordered the creation of a risk-based deposit insurance assessment scheme. Brokered deposits and the solicitation of deposits were restricted, as were the non-bank activities of insured state banks. FDICIA created new supervisory and regulatory examination standards and put forth new capital requirements for banks. It also expanded prohibitions against insider activities and created new Truth in Savings provisions.

Sec. 302 of the Act is provides for risk-based assessments. The Board of Directors shall, by regulation, establish a risk-based assessment system for insured depository institutions. The Board of Directors may establish separate risk-based assessment systems for large and small members of each deposit insurance fund

BS 7799

BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and after several revisions, was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000. ISO 17799 was most recently revised in June 2005 and is expected to be renamed ISO/IEC 27002 during 2007.

A second part to BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use." BS 7799-2 focused on how to implement an Information security management system (ISMS), referring to the information security management structure and controls identified in ISO 17799. The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA) (Deming quality assurance model), aligning it with quality standards such as ISO 9000. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.

BS 7799-3:2005: Information Security Management Systems - Guidelines for Information Security Risk Management was issued in 2005. It gives guidance to support the requirements given in ISO 270015 regarding all aspects of an ISMS risk management cycle.

Risk assessment is fundamental to developing an ISMS that meets the requirements of ISO 27001:2005 (BS7799-2).

And identifying, evaluating, treating and managing information security risks are key processes if businesses want to keep their information safe and secure. Whilst these processes are specified in the new information security standard BS ISO/IEC 27001:2005, further guidance is required on how to manage these risks as well as to put them in context with other business risks.

BS 7799-3:2006 was published on 16 March 2006. The new British Standard – BS 7799-3:2006– provides this guidance and covers:

- Risk assessment
- Risk treatment
- Management decision making
- Risk re-assessment
- Monitoring and reviewing of risk profile
- Information security risk in the context of corporate governance
- Compliance with other risk based standards and regulations

BS 7799-3:2006 gives guidance to support the requirements given in BS ISO/IEC 27001:2005 regarding all aspects of an information security management system (ISMS) risk management cycle. This includes assessing and evaluating the risks, implementing controls to treat the risks, monitoring and reviewing the risks, and maintaining and improving the system of risk controls.

The focus of this standard is effective information security through an ongoing programme of risk management activities. This focus is targeted at information security in the context of an organization's business risks.

The guidance set out in this British Standard is intended to be applicable to all organizations, regardless of their type, size and nature of business. It is intended for those business managers and their staff involved in ISMS risk management activities.

Basel II

Basel II is the second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.

The final version aims at:

1. Ensuring that capital allocation is more risk sensitive;
2. Separating operational risk from credit risk, and quantifying both;
3. Attempting to align economic and regulatory capital more closely to reduce the scope for regulatory arbitrage.

Basel II uses a "three pillars" concept – (1) minimum capital requirements (addressing risk), (2) supervisory review and (3) market discipline – to promote greater stability in the financial system.

The Basel I accord dealt with only parts of each of these pillars. For example: with respect to the first Basel II pillar, only one risk, credit risk, was dealt with in a simple manner while market risk was an afterthought; operational risk was not dealt with at all.

On July 4, 2006, the committee released a comprehensive version of the Accord, incorporating the June 2004 Basel II Framework, the elements of the 1988 Accord that were not revised during the Basel II process, the 1996 Amendment to the

Capital Accord to Incorporate Market Risks, and the November 2005 paper on Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework. No new elements have been introduced in this compilation. This version is now the current version.

This Framework will be applied on a consolidated basis to internationally active banks.

The scope of application of the Framework will include, on a fully consolidated basis, any holding company that is the parent entity within a banking group to ensure that it captures the risk of the whole banking group. Banking groups are groups that engage predominantly in banking activities and, in some countries, a banking group may be registered as a bank.

The Framework will also apply to all internationally active banks at every tier within a banking group, also on a fully consolidated basis (see illustrative chart at the end of this section). A three-year transitional period for applying full sub-consolidation was provided for those countries where this was not currently a requirement.

As one of the principal objectives of supervision is the protection of depositors, it is essential to ensure that capital recognised in capital adequacy measures is readily available for those depositors. Accordingly, supervisors should test that individual banks are adequately capitalised on a stand-alone basis.

The First Pillar presents the calculation of total minimum capital requirements for credit, market and operational risk.

The Second Pillar discusses the key principles of supervisory review, risk management guidance and supervisory transparency and accountability with respect to banking risks, including guidance relating to, among other things, the

treatment of interest rate risk in the banking book, credit risk (stress testing, definition of default, residual risk, and credit concentration risk), operational risk, enhanced cross-border communication and cooperation, and securitisation.

The Third Pillar lays down the general considerations and the disclosure requirements.

Code of Federal Regulations – Title 21 part 11 [FDA CFR 21 part 11]

The Code of Federal Regulations (CFR) is a codification of the general and permanent rules published in the Federal Register by the Executive departments and agencies of the Federal Government. Title 21 of the CFR is reserved for rules of the Food and Drug Administration. Part 11 is the final rule on electronic records and electronic signatures.

In 1991, members of the pharmaceutical industry met with the agency to determine how they could accommodate paperless record systems under the current good manufacturing practice (CGMP) regulations in parts 210 and 211 (21 CFR parts 210 and 211). FDA created a Task Force on Electronic Identification/Signatures to develop a uniform approach by which the agency could accept electronic signatures and records in all program areas. In a February 24, 1992, report, a task force subgroup, the Electronic Identification/Signature Working Group, recommended publication of an advance notice of proposed rulemaking (ANPRM) to obtain public comment on the issues involved. After receiving and considering comments, the final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or

agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

The FDA in conjunction with their new GMP initiative has issued a draft guidance document outlining their new approach to the scope and applicability of 21 CFR Part 11. This approach is based on the FDA's risk-based assessment for regulatory compliance: A Risk-Based Approach to Pharmaceutical Current Good Manufacturing Practices (cGMP) for the 21st Century.

Standards/best practices

Companies which do not have a framework in place to execute continuous process improvement are likely to treat clause 49, Sarbanes-Oxley and Basel II requirements as a one-time project (a project which just integrates the minimum requirements of the regulations) or as one more just-in-time audit activity. But if a company makes compliance a best practices strategy, then that means alignment across the organization for people, processes and technology. Hence, the regulations become a part of the risk management philosophy that uses the best aspects of the standard/best practices.

The relevant standards/best practices are discussed in brief as under:

COBIT

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance, security and control in a company.

It includes the assessment and management of IT risks. Recently, ISACA has released Val IT, which correlates the COBIT processes to senior management processes required to get good value from IT investments.

COBIT is fast becoming one of the key standards used by corporations around the globe who need a well-defined set of policies regarding internal control over information and related IT systems. COBIT is compliant with other standards, such as COSO and ISO 17799, and contains 34 high-level control objectives along with over 300 detailed control objectives.

Essentially, COBIT represents an authoritative, up-to-date control framework, a set of generally accepted control objectives, along with a complimentary product that allows the straightforward application of the Framework and Control Objectives - called the Audit Guidelines. COBIT applies to enterprise-wide information systems, such as personal computers, mini-computers, mainframes and distributed environments. Since the 1st edition of COBIT was released in 1996 it has been sold and implemented in over 100 countries throughout the world.

ISO

The International Organization for Standardization (ISO) (in French; *L'Organisation internationale de normalisation*) is an international standard-setting body composed of representatives from various national standards bodies. Founded on 23 February 1947, the organization produces world-wide industrial and commercial standards. These are ISO 1–ISO 999, ISO 1000–ISO 9999, ISO 10000–ISO 19999 and ISO 20000–ISO 29999.

ISO 17799

First published as a code of practice in the United Kingdom, it was renamed BS 7799 and published in 1995. Initially, there was not much acceptance due to a number of pressing IT issues, such as the coming Y2K compliance. A major overhaul was conducted in 1999, resulting in it being published as an ISO standard in December 2000. ISO 17799 is a comprehensive set of controls comprising best practices in information security. Its main intention is to serve as a reference point for identifying a range of controls that are needed for situations where information systems are used in industry and commerce. The standard consists of eleven sections, as opposed to just ten in the 2000 standard editions. They are the following:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. HR Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information System acquisition, development and maintenance
9. Information Security Incident Management
10. Business Continuity

11. Compliance

AS/NZS 4360

The Australian/New Zealand standard for risk management provides a generic guide for managing risks. This Standard specifies the elements of the risk management process, but it is not the purpose of this Standard to enforce uniformity of risk management systems. It is generic and independent of any specific industry or economic sector. The design and implementation of the risk management system will be influenced by the varying needs of an organization, its particular objectives, its products and services, and the processes and specific practices employed.

This Standard should be applied at all stages in the life of an activity, function, project, product or asset. The maximum benefit is usually obtained by applying the risk management process from the beginning.

CMMI

Capability Maturity Model Integration (CMMI) is a process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

Risk management is a required Process Area (PA) at Level 3 of the Capability Maturity Model Integrated (CMMI), so it is necessary to have effective risk management processes in place to qualify for Level 3 in the Staged representation. Level 1 organizations can practice some rudimentary forms of risk management (e.g., identifying risks, using action items to manage them); however, be aware that any project which, for example, fails to adequately manage action items or problems is also likely to have difficulty managing risks.

The model contains a Risk Management Maturity Model. The RMMM is designed as a diagnostic tool instead of a prescriptive model for implementation.

The Software Engineering Institute (SEI) at Carnegie-Mellon University has developed a Capability Maturity Model (CMM) for Software organizations and one (CMMI) for Systems Engineering organizations. These models define five levels of increasing capability and maturity, termed Initial (Level 1), Repeatable (Level 2), Defined (Level 3), Managed (Level 4) and Optimizing (Level 5). Each level is clearly characterized and defined, enabling organizations to assess themselves against an agreed scale. Having discovered its CMM level, an organization can then set clear targets for improvement, aiming towards the next level of capability and maturity.

SAS 70-2

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) in 1992.

A service auditor's examination performed in accordance with SAS No. 70 is widely recognized, because it represents that a service organization has been

through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. The issuance of a service auditor's report prepared in accordance with SAS No. 70 signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 does not specify a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 Audit is not a "checklist" audit.

SAS No. 70 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that impact a user organization's system of internal controls could be application service providers, bank trust departments, claims processing centers, data centers, third party administrators, or other data processing service bureaus.

The user auditor may need to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk.

The standard is used to report on the "processing of transactions by service organizations," which can be done by completing either a SAS 70 Type I or Type II audit. A SAS 70 Type I is known as "reporting on controls placed in operation". It describes the service organization's description of controls at a specific point in time. A SAS 70 Type II is known as "reporting on controls placed in operation" and "tests of operating effectiveness." It not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period. The contents of each type of report are described in the following table:

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of	Optional	Optional

terms).		

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

ITIL

The Information Technology Infrastructure Library (ITIL) is a framework of best practice approaches intended to facilitate the delivery of high quality information technology (IT) services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both high financial quality and value in IT operations. These procedures are supplier-independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.

Six Sigma

At many organizations Six Sigma simply means a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects (driving towards six standard deviations between the mean and the nearest specification limit) in any process – from manufacturing to transactional and from product to service.

Bibliography

1) **http://www.garp.com/**

The Global Association of Risk Professionals (GARP) is a not-for-profit association consisting of **55610** individuals around the world who are involved in financial risk management. GARP's aim is to encourage and enhance communications between risk professionals, practitioners and regulators worldwide. Through its events, publications, website and certification examination (FRM), GARP works on expanding views and increasing recognition of the global risk management community.

2) http://www.cmra.com/

Capital Market Risk Advisors (CMRA), is the preeminent financial advisory firm specializing in risk management, hedge funds and derivatives.

CMRA provides institutional investors, funds of funds, hedge fund managers, mutual funds, traditional money managers, banks/investment banks, and law firms with consulting services

3) http://www.iiaindia.org/

The Institute of Internal Auditors - India is affiliated to its parent body in Florida, USA which provides Internal Auditing Practitioners, Executive Management, and Board of Directors with standards, guidance and information on best practices. The Institute also conducts the Certified Internal Auditor exam, which is the hallmark of excellence in internal auditing worldwide.

4) http://www.auditnet.org/

Kaplan's AuditNet Resource is a comprehensive list of Internet resources for auditors and accountants available on the Internet via email, ftp, newsgroups, Listserv, and the World Wide Web. In August 1994, Jim Kaplan, the Author of The Auditor's Guide to Internet Resources, began distributing the AuditNet Resource List to financial professionals around the world. The primary audience for the resources is practicing auditors, accountants and financial professionals.

5) http://www.coso.org/

The Committee of Sponsoring Organisations of the Treadway Commission (COSO), which includes The IIA, offers an informational Web site, www.coso.org. COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

6) **http://www.theiia.org/**

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association of more than 117,000 members with global headquarters in Altamonte Springs, Fla., United States. Throughout the world, The IIA is

recognized as the internal audit profession's leader in certification, education, research, and technological guidance.

7) **http://www.corpgov.net/**

Since 1995 the Corporate Governance site has provided news, internet links, and a small reference library. Corporate Governance serves as a discussion forum and network for stakeholders who believe active participation by shareowners in governing corporations will enhance their ability to create wealth.

8) http://www.rmis.com/sites/rismanag.htm

Provides links to other risk management sites and articles of use for people looking for material on Risk Management.

9) http://www.ecgi.org/

The ECGI is an international scientific non-profit association. They provide a forum for debate and dialogue between academics, legislators and practitioners, focusing on major corporate governance issues and thereby promoting best practice

10) http://www.auditserve.com

The Worldwide Connection for Audit, Security, Control and Euro Project Professionals

11) http://www.riskworld.com/

This web-site offers news articles, briefs and reports on risk analysis, assessment and management

12) http://riskcenter.com

RiskCenter is a news service devoted exclusively to providing financial risk professionals with the inside scoop on breaking economic, political and financial stories, as well as the risk strategies required to measure and manage these risks.

13) http://www.riskinstitute.ch/

Web site of International Financial Risk Institute (IFRI)

14) http://www.gloriamundi.org/

GloriaMundi was conceived and created by Barry Schachter in 1996 to collect information on the latest developments in Value at Risk for a research project of his own. However, soon after, he began receiving email from people who had found the site and who had questions about VaR or suggestions for the site. The site serves as a resource for the community of individuals interested in Value at Risk and more generally financial risk management.

15) http://www.irgc.org/

The International Risk Governance Council (IRGC) is an independent foundation established in 2003 under Articles 80 and thereafter of the Swiss Civil Code.

IRGC's focus and raison d'être is to help improve the anticipation and governance of global, systemic risks.

IRGC is a public-private partnership in which governments, industry and academia can freely discuss such issues and, together, design and propose appropriate risk governance recommendations that have relevance to both developed and developing countries.

16) http://www.iso.org/

International organization for Standardization- network of the national standards institutes of 156 countries,

17) http://www.casact.org/

The Casualty Actuarial Society is a professional organization whose purpose is the advancement of the body of knowledge of actuarial science applied to property, casualty, and similar risk exposures.

18) http://www.sebi.gov.in

Securities and Exchange Board of India