Chapter 1: INTRODUCTION

Chapter Highlights

This chapter presents the progressive development in Risk Management thinking by examining the various Reports and Directives by contemporary major contributors in the field of Risk Management from various industries globally. The salient feature of this chapter is to elucidate the impact and prominence of these publications & promulgations in risk management, internal control internal auditing, and corporate governance in organizations. Currently, Enterprise Risk Management (ERM) is a globally accepted and growing field. As a result, a number of risk frameworks and statements have been published by professional organizations around the world. The most commonly used starting point for implementing an ERM initiative is the COSO ERM framework which was promulgated by the Committee of Sponsoring Organization's of the Treadway Commission (USA) in 2004, following the various corporate scandals and the mandatory implementation of The Sarbanes-Oxley Act (SOX) in some parts of the globe. This chapter further attempts to uncover the wide-ranging implications for risk management and, thus, corporate governance. Finally the chapter concludes on the key drivers and trends in Enterprise Risk Management that is driving growth in, and acceptance of ERM to explore further literature in subsequent chapters.

Contents

1.0 Evolution of the Enterprise Risk Management System paradigm

While studying the Body of Management Knowledge, one of the distinguished management history gurus stated that, *'Within the practices of the past there are lessons of history for tomorrow in a continuous stream. We occupy but one point in this stream. The purpose is to present the past as a prologue to the future'* (Daniel A. Wren, 2004).

In these above captivating lines, the present day modern management thinking in Risk Management has evolved from a whole range of influences over a period of time. By examining the backgrounds, ideas and influences of contemporary major contributors in the field of Risk Management, a vignette into the evolution of the management thinking within the precincts of the *Board Room* on corporate risk management principles is presented below.

Risk Management is one of those concepts wherein almost everyone will agree that one must have a good risk management system or program in place. But these same professionals have difficulty when pressed for a better definition of ***risk management*** and for an appropriate method. The lack of consistent understanding of risk management has until recently been similar to the earlier lack of general understanding of the ubiquitous management term ***internal control***. There was no widely accepted definition for internal control or what exactly was meant by this management expression. Internal Control was widely discussed in the United Kingdom, United States of America, Australia and Canada at Board Room level and operational levels.

In the early 90s, in the US, the Committee of Sponsoring Organisation's (COSO) released its Internal Control framework that has a widely recognized definition of internal controls for all organizations thereby addressing the problem towards defining internal control. In late 2004, COSO had also released a new definition or risk management framework called COSO Enterprise Risk Management framework or popularly known as COSO ERM framework to address the problem towards defining risk management. Enterprise Risk Management (ERM) is a globally accepted and growing field. As a

result, a number of risk frameworks and statements have been published by professional organizations around the world. Some of the publications urge businesses to use these frameworks. While a variety of ERM frameworks have been suggested by different professional bodies and management consultants, the essential components of most frameworks are similar excepting ERM process and the specific steps (Walker & Shenkir, 2006). 'The most commonly used starting point for implementing an ERM initiative is the COSO ERM framework (EuropeanCEO, 2001). ERM no doubt is a hot topic and a contemporary area in the traditional risk management discipline; and COSO ERM is being widely used in many organizations globally in the Banking sector, Insurance sector, Hospital sector, Pharmaceutical sector, Energy sector to name a few (Deloitte, 2008). The COSO ERM concepts are important for all levels of the organization and give a holistic view of risk management.

GENERAL INDUSTRY	FINANCIAL INDUSTRY	INSURANCE INDUSTRY
❑ *Cadbury Report (UK), 1992*	❑ *Basel I Accord, (Europe), 1988*	❑ *Solvency I Directive, (Europe), 1970*
❑ *Dey Report (Canada), 1994*	❑ *OSFI (Canada)*	❑ **Solvency II Directive, (Europe), 2002**
❑ *Australia/New Zealand Risk Management Standard, 1995*	❑ *FSA (UK)*	
❑ *Kon TraG (Germany), 1998*	❑ *King II Report (South Africa), 2002*	
❑ **Turnbull Report (UK), 1999**	❑ **Basel II Accord, (Europe), 2004**	
❑ **Sarbanes Oxley Act (USA), 2002**		

RATING AGENCIES
❑ *Moody's*
❑ **Standard & Poor's**

Table 1.1, Regulatory Drivers to Enterprise Risk Management (Source: Various articles)

Following the series of scandals in corporate America, the Sarbanes-Oxley Act (SOX) of 2002 has had a further impact on how organizations should use and adapt the COSO ERM. SOX has established strong requirements on internal controls, governance and risk

management thereof. Presented below (Table 1.1) are the corporate governance guidelines, regulatory and rating agencies requirements; from various countries and business sectors.

The most prominent and relatively contemporary drivers, that have profoundly articulated the significance of internal control and corporate governance, in order to propel the current Enterprise Risk Management System Framework as promulgated by COSO are elucidated further to get an overview of the Body of Management Knowledge, so as to present the past as a prologue to the future.

1.1 The Turnbull Report

A forerunner to the currently widely known Enterprise Risk Management system was proposed earlier on by the *Turnbull Report (1999)* which originated in the United Kingdom, coming from the position of 'enhanced internal controls'. The committee which wrote the report was chaired by Nigel Turnbull. 'Turnbull Report' is a report drawn up with the London Stock Exchange (LSE) for listed companies and was titled *'Internal Control: Guidance for Directors on the Combined Code'* (1999). The report informs Company Directors of their obligations under the Combined Code on Corporate Governance with regard to best practice on internal control, audits, financial and management reporting.

The Combined Code on Corporate Governance also referred as just 'the Combined Code' is a set of principles of good corporate governance and provides a code of best practice aimed at companies listed on the LSE. In the early 90s, in response to the various major corporate scandals associated with governance failures in the UK, many reports were published and business codes were established. The Combined Code on Corporate Governance is fundamentally a consolidation and refinement of a number of different reports and codes concerning opinions on good corporate governance. Therefore, the Combined Code adopts a 'principles-based-approach' by providing only general

guidelines of best practice vis-à-vis a 'rules-based-approach' which rigidly defines exact provisions and compliance that must be adhered to in the business.

Turnbull Report was also recommended by professional bodies for good risk management and internal control especially for getting added value in their company. The principles-based approach afforded the flexibility in the process that need to be followed. In essence, the process that needs to be followed must fit the circumstances of the company. Directors may therefore decide that only some of the suggested practices are appropriate to their circumstances.

Impact of Turnbull Report on risk management

In order to achieve Turnbull, companies have to adopt a risk-based approach to establishing a system of internal control and reviewing its effectiveness. The benefits and consequences of Turnbull was that it just makes sound business sense to manage risk effectively and also to embed internal control in the business processes by which a company pursues its corporate objectives. Anthony Carey, Project Director, Turnbull Report has commented on the report in various management journals. A snap shot of what he describes is presented below highlighting the significance of the evolutionary path taken to arrive at the current ERM principles.

According to Carey (2000), Turnbull's Report emphasizes on the good business practice in the areas of risk management and control in the following steps.

- Emphasize that a company's internal control system has a key role to play in the management of risks that are significant to the fulfillment of its business objectives.
- Focus should be on the significant risks that could blow the company off track.
- Control system must be linked to managing in an effective manner the risks an organization consciously decides to carry.

Turnbull is not about eliminating risks, per se. Nevertheless, it illuminates on the following facets (Carey, 2000):

- **Benefits of managing risk effectively**

  Managing risk effectively can make an organization more flexible and responsive to its external environment, enabling it to satisfy customers' ever-changing needs more fully; gain an early-mover advantage while leading an enhanced reputation in medium and long term. Boards of Directors are concerned with the long-term direction of their organizations. They need to set goals with varying timeframes. The impact of various risks crystallizing can be that the organization's realized goals are very different from the intended, desired ones. Therefore managing risks effectively is the key to organizational success.

- **Identifying the risks**

  The shortcoming due to risk identification overload has been highlighted as this can prevent the significant risks being given appropriate attention. If lots of risks have traditionally been identified, they can usefully be analyzed on the basis of relevance to meeting the business objectives and to highlighting areas where new objectives may be needed. It is particularly useful to relate them to the likely obstacles to achieving the critical success factors associated with the achievement of the organization's objectives. Focusing on 'killer-risks' is crucial rather than having 1001 risks regardless of the likelihood that they will occur or the impact they would have if they did materialize.

- **Prioritizing the risks**

  The gross risk associated with an event is assessed, that is the probability and impact of an event happening on the assumption that control processes are very weak or non-existent. Risks are then prioritized according to their impact and likelihood of occurrence. The impact should be considered not merely in financial terms but more importantly in terms of potential effect on the achievement of the organization's objectives. Not all risks will be identified as significant. Non-significant risks should be reviewed regularly, particularly in the light of changing external events, to check that they remain non-significant.

- **Managing the significant risks**

  Having identified and then prioritized the significant risks in gross terms, it is then helpful to determine for each of them the risk ownership at Board level, control strategy, accountability for managing risk, monitoring residual risks and early warning mechanism.

- **An organization wide, total risk management approach**

  Turnbull has promulgated the idea of not having the delegation of risk management to a single individual unlike the traditional Silo based Risk Management. Delegation should ideally be spread across those responsible for managing different organizational activities. While at the top, the Board of Directors should set appropriate internal control policies and seek regular assurance that the control system is functioning effectively. Furthermore, it is for the Board to decide upon the organization's Risk Appetite. This role is played by the Internal Auditors. Similarly, Line Management's job is to design, operate and monitor a system that reflects the Board's policies.

Achieving Turnbull: ***A catalyst for performance improvement***

There has been much discussion in the business community and the media about Turnbull's likely impact in the coming years. Although the primary purpose is to provide guidance to help LSE listed companies to implement the internal control requirements of the Combined Code, the report has been a catalyst for performance improvement in various business houses (Carey, 2000) including good risk management. Good risk management has the potential to re-orient the whole organization around performance improvement. Turnbull provides the opportunity to improve, not only the management of risk, but also the organization as a whole.

It has been observed that many American management pundits do not to seem to discuss much on achieving Turnbull, nevertheless, the close coupling between internal control and risk management in the Turnbull Report echoes similar developments across the

Atlantic in the US and Canada wherein other influential reports have emphasized the importance of risk management as well as internal control.

1.2 The Basel Accords

According to Walker and Shenkir (2006), Basel framework is designed to improve the international banking system and make it stronger. The framework is a focused on maintaining consistent capital adequacy requirements among banks. A key idea behind the framework is that banks should match capital to the actual level of risks and to set minimum capital levels.

The Basel Accord refers to the banking supervision Accords (recommendations on banking laws and regulations). Basel I and Basel II issued by the Basel Committee on Banking Supervision (BCBS), Basel, Switzerland. The role of ERM has been brought into focus for the Banking Industry through the Basel Capital Accord (1988) and a modified version known as Basel II (2001). The Basel Capital Accord introduced a 'risk-based approach to regulation' using the Value at Risk (VaR) method of assessing risk. It established capital requirements equal to a specified percentage of the value of the bank's assets, classified into four groups according to type and degree of risk. Basel II accepts the use of a number of different risk metrics including internally produced risk measures and assessments by rating agencies.

In order to provide background information on the risk control philosophy of the Basel Accords, key financial risks covered in the standard are defined below. Financial risks include market risk, credit risk and operational risk.

- **Market risk** is defined as the risk of losses due to movements in financial market prices or volatilities (Jorion, 2005).
- **Credit risk** is defined as the risk of losses due to the fact that counterparties may be unwilling or unable to fulfill their contractual obligations (Jorion, 2005).
- **Operational risk** is defined as the risk of loss resulting from failed or inadequate internal processes, systems, and people, or from external events (Jorion, 2005).

Often, however, these three categories interact, so that any classification is to some extent arbitrary.

Basel I Accord

It refers to a round of deliberations by central bankers from around the world, and in 1988, BCBS published a set of minimal capital requirements for banks. It is also known as the '1988 Capital Accord.'

Leech (2003) states that the Basel Committee, part of the Bank for International Settlements, has been working since 1998 on the development of a new corporate governance framework to address what they consider to be an ineffective and broken ***corporate governance*** regime. They came up with Basel Capital Accord II. Basel identified a list of key governance deficiencies present in banks in countries all over the world that have been involved in significant frauds and/or control breakdowns. Many of the corporate governance problems identified by Basel in banks globally have also been present in corporate sector disasters including Enron, WorldCom, Allied Irish Bank, HealthSouth, and others.

Basel II Accord

According to Hashagen (2008), Basel I addressed market and credit risks, but Basel II changes the treatment of credit risk and requires that banks have enough capital to cover operational risks. It also imposes qualitative requirements on the management of all risks as well as new disclosures. To be able to implement sound Basel II, most banks will need to rethink their business strategies in relation to the risks that underlie them. Calculating capital requirements under the New Accord ***requires a bank to implement a comprehensive risk management framework*** across the institution. The risk management improvements that are the intended result may be rewarded by lower capital requirements. Three guiding principles (called Pillars) form the new framework as shown in Fig. 1.1. The *'three pillars'* concept of Basel II is presented:

Pillar 1

Minimum capital requirements (addressing risk):- Deals with the methodologies to arrive at minimum capital requirement for credit risk, operational risk and market risk.

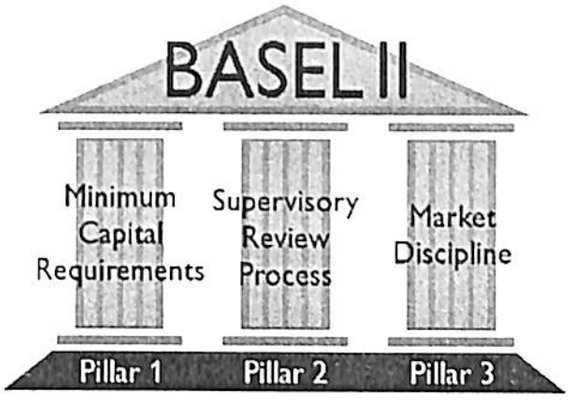

Fig. 1.1: Three Pillars in Basel II Accord
(Source: Basel II)

Pillar 2

Supervisory review:- Deals with the supervisory review process which is guided by the principle that banks must have risk control and management processes that are adequate to their business structure and risk profile. Supervisory review would be in the form of onsite inspections, offsite reviews, discussions with the bank's management, review of work done by external auditors, etc.

Pillar 3

Market discipline (to promote greater stability in the financial system):- Deals with market disclosure and the purpose is to impose market discipline in order to reinforce minimum capital requirements, impose incentives for firms that behave prudently and promote safety and soundness in banks and financial systems. This requires significant amount of additional information that needs to be disclosed.

Basel II was initially published in 2004, to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

- Advocates of Basel II believe that such an international standard can help protect the international financial system from the types of problems that might arise should a major bank or a series of banks collapse. In practice, Basel II attempts to accomplish this by setting up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. Generally

speaking, these rules mean that the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability.

- Opponents of Basel II believe that the artificially high capital requirements and a costly compliance burden would reduce competitiveness and lead to inefficient use of capital.

For institutions worldwide, Basel II compliance is a risk management challenge with strategic business implications. Even those institutions that are not required to comply with the New Accord will likely tend to use its advanced requirements as risk management and economic capital benchmarks so they may remain competitive with those that must comply (Hashagen, 2008).

Basel III Accord

Many reports acknowledge that the deadline (2008) for implementing the international banking reforms i.e., Basel II is approaching fast, but already Basel III is being discussed. After Basel II comes Basel III earmarked for 2020 compliance deadline.

Impact of Basel II Accord on risk management

According to Hashagen (2008), the Basel Committee for Banking Supervision, of the Basel II Capital Accord has evolved as a complex set of recommendations that will create a variety of regulatory compliance challenges for banks around the globe. More important, however, are the wide range of business implications and risk-management challenges that the revised framework for International Convergence of Capital Measurement and Capital Standards (the New Accord) will trigger for banks, their non-bank competitors, customers, rating agencies, regulators, and, ultimately, the global capital markets. The implications are:

(1) Banks will be asked to implement an ***enterprise-wide risk-management framework*** that ties regulatory capital to economic capital.

(2) ***Non-banks*** outside the scope of Basel II will not face its compliance challenges but ***might be pushed to use it as a competitive benchmark***.

(3) Banks will need to collect and disclose new information and face the implications of increased transparency.

(4) ***Rating agencies have new prominence*** as a result of the Basel II framework and could experience new competition.

(5) Regulators are challenged to provide a level playing field in their jurisdictions and internationally as the Basel Committee's recommendations are implemented by legislatures in various countries.

(6) The global banks could experience extended trends toward increased securitization as financial institutions adapt to Basel II requirements.

(7) The data requirements of Basel II are substantial, the New Accord is not simply a data and information systems exercise. Ultimately, Basel II's capital requirements ***have wide-ranging implications for risk management*** and, thus, ***corporate governance.***

(8) It also encourages ongoing improvements in ***risk measurement, assessment,*** and ***mitigation***. It presents banks with an opportunity to gain competitive advantage by allocating capital to those processes, segments, and markets that show a strong risk/return ratio.

(9) Greater emphasis on ***Internal Auditing*** - intended to improve safety and soundness in the financial system by placing increased emphasis on banks' own internal control and risk-management processes and models, the supervisory review process, and market discipline.

1.3 The Solvency II Directive

The actuarial profession has transformed to meet the needs of ERM in a global way. This has been corroborated by many literatures in the Actuarial Research fraternity, including reviews from Casualty Actuarial Society, USA.

Solvency II is a set of regulatory requirements for insurance firms that operate in the European Union. Solvency II is somewhat similar to the banking regulations of Basel II and is also called 'Basel for insurers' or 'counterpart for Basel II'. Solvency II is based on a three-pillar approach involving a basic minimum capital requirement, proactive solvency management and emphasis on disclosure. The International Association of Insurance Supervisors (IAIS) published a statement of 'Principles of Capital Adequacy and Solvency' in 2002. This statement included requirements that capital adequacy and solvency regimes be supplemented by risk management systems, and the matching of assets and liabilities. The IAIS statement of Insurance Core Principles requires insurers to recognize the range of risks and to assess and manage them effectively. It also requires insurers to undertake regular stress testing for a range of adverse scenarios to assess the adequacy of reserves. A feature of ERM is the quantification of risk. Furthermore, ERM affects enterprise-wide cash flow for strategic investments.

1.4 The Sarbanes-Oxley Act

Across the Atlantic the American business community was also confounded with major corporate scandals and accounting scandals. The bright future as predicted by economists like Schwartz et al (1997) who then stated that *'there would never be another recession'* went wrong with the collapse of the dot-com bubble of the late 90s. During this entire period of time, some companies started 'cooking their books' all along stretching their accounting rules. Perhaps the most egregious of these corporations was Enron, an aggressively diversified company, but started as an Oil & Gas Pipeline operator.

However, Enron was not alone, as many other business houses too had similar flagrant management practice. Fraudulent accounting, poor governance practices of Board of Directors, improper risk management and failure of internal auditors were the reasons for declaring bankruptcy lastly. The United States federal law enacted in 2002 in response to number of such scandals 'The Sarbanes-Oxley Act of 2002' also known as the 'Public Company Accounting Reform and Investor Protection Act of 2002' and commonly called

'SOX' or 'SarBox'. The main architects of this Act were Senator Paul Sarbanes and Representative Michael Oxley.

In the US, SOX is mandatory and all organizations must comply with the legislation. SOX has introduced major changes to the regulation of financial practice and corporate governance. SOX is arranged into 'titles' ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. It should be noted that much of the SOX text mandates rules to be issued by the responsible agency, the SEC. That is, SOX states that a rule should be established, and the SEC sets the rules later. Therefore, the upcoming specific SOX rules to be developed by the SEC may or may not be significant to most.

Study by McKinsey & Company (2007) debates over the perceived benefits and costs of implementing SOX and it states that:

- *SOX supporters* contend that the legislation was necessary and has played a useful role in restoring public confidence in the nation's capital markets by, among other things, strengthening corporate accounting controls.
- *SOX opponents* of the bill claim that it has reduced America's international competitive edge against foreign financial service providers, claiming that SOX has introduced an overly complex and regulatory environment into U.S. financial markets.

SOX sets a number of deadlines for compliance. Although SOX established various other provisions, the following salient features are highlighted below:

- Established new regulatory rules for Public Accounting.
- Established Financial Auditing Standards, Enhanced Auditor independence.
- Established regulatory rules for Corporate Governace.
- Covered issues such as Public Company Accounting Oversight Board (PCAOB).
- Enhanced Internal control assessment, Enhanced Financial disclosure.
- Indirect dependency on Enterprise Risk Management (ERM).

Through SOX, the public accounting profession was transformed. The American Institute of Certified Public Accountants (AICPA's) Auditing Standards Board lost its responsibility for setting public corporation auditing standards and the rules soon changed for Corporate Senior Executives, Boards of Directors and their Audit Committees.

A new entity, an overarching Public Company Accounting Oversight Board or PCAOB was also established under the SEC to set financial reporting and auditing standards as well as to oversee individual public accounting firms. Although not directly covered in the corporate governance legislation, SOX has also very much impacted enterprise risk management practices.

PCAOB is a private-sector, non-profit corporation created by the Sarbanes-Oxley Act, to oversee the auditors of public companies. Its stated purpose is to 'protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports'. PCAOB is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as 'auditors of public companies'.

Impact of SOX in a global scale

Since becoming a US law in 2002, the SOX has had a major impact on worldwide enterprises and particularly those with securities registered through the SEC. SOX has changed the public accounting regulatory landscape from one of 'self regulation by external audit firms' to 'quasi-governmental rules for public accounting firms'. More importantly, SOX globally requires Business Managers to take personal responsibility for the documentation, review, and testing of their enterprise's internal controls Moeller (2007).

The drivers of any legislation is often due to political and economic events; and those laws and rules often stay for a long time even after the underlying problems have been corrected. On similar lines, Moeller (2007) thinks that SOX will be with all business

professionals for a long time into the future. A cue to be taken from that statement is that enterprise-wide risk management systems are also going to play its role as long as it makes good business sense through SOX implementation.

Furthermore, SOX is the most important financial legislation passed in the US since the early 1930s, and it has caused changes for Internal Auditors, External Auditors, Risk Managers, Financial Managers, Boards of Directors and Corporate Governance Administrators. While SOX is directed at companies with SEC registered securities, its concepts, if not actual rules and processes, encompass a wider swath of worldwide enterprises. The overall SOX rules are very important to all parties involved with implementing an effective enterprise wide risk management program.

Impact of SOX on risk management

Moeller (2004), states that ***SOX requires enterprises to follow the Committee of Sponsoring Organisations (COSO) internal control rules, the COSO Enterprise Risk Management (ERM) was released after SOX that is not specifically mentioned in the legislation.*** Nevertheless, both SOX and COSO ERM have some important dependencies on one another. Furthermore, the titles which are most important for risk management and specifically supporting the ERM philosophy are:

- SOX Section 404 : Management's Assessment of Internal Controls
- SOX Section 302 : Corporate Responsibility for Financial Reports

SOX Section 404 requires that all impacted enterprises must document and describe their key internal controls and then must test those controls to determine if they are operating effectively as defined and also must identify any material weaknesses in those internal controls. Enterprise management then provides this formal assessment of internal controls to their external auditors who review the work, perform additional tests themselves as they may feel necessary, and use this overall assessment of internal controls to provide their audited opinion on the fairness of the published statements. This

is a major element of SOX, and management also is required to formally assert that their internal controls are adequate. This exemplifies the role of the Internal Auditors.

Going further forward, enterprise has to establish processes for continuous monitoring, evaluation and controls improvement including addressing control gaps. Simply put, the management is now required to report on the *'quality of their internal controls'* and the public accounting firm responsible for the financial statement audit must attest to the adequacy and accuracy of that management prepared internal accounting controls report. Management has always been traditionally responsible for preparing their periodic financial reports, and their external auditors previously only reviewed those financial numbers and certified that they were *'fairly stated'* as part of the audit. Now with SOX implementation, management is responsible for documenting and testing their internal financial controls in order to prepare a report on their very own effectiveness. The external auditors now review the supporting materials leading up to that internal financial controls report to assert that the report is an accurate description of that internal control environment.

To the non-auditor, this might appear to be an obscure and almost trivial requirement. Even some internal auditors that primarily specialize in operational audit review may wonder about the nuances in this process.

In order to launch Section 404, Internal Audit and Risk Management function contribute extensively in identifying key processes, organizing the internal control review, identify, document and test key internal controls.

SOX Section 302 instills corporate responsibility for financial reports. If an enterprise is caught filing financial reports with fraudulent numbers, technically neither CEO nor CFO takes responsibility. The matter gets pushed down the corporate ladder. SOX 302 has raised the bar by making the CEO and/or CFO to certify the quarterly and annual reports and take responsibility. Given the criminal penalties associated to SOX non compliance, the signer requirement has placed a significantly enormous burden on the CEO/CFO.

This finally boils down to risk monitoring and reporting process. Therefore, the risk or ERM function, including internal audit function can often act as an internal consultant and help top management establish effective processes here.

To establish an environment as stated above, Risk Management and Internal Audit must place a strong emphasis on performing reviews surrounding significant internal control areas. This is usually done through a detailed risk assessment of the internal control environments, discussions of these assessments with the Board, and then a detailed plan documenting how these internal control systems will be reviewed.

Many risk assessment and/or internal audit reports may identify significant weaknesses in areas of the enterprise that are not material to overall operations. Similarly, Internal Audit and Risk function need to work closely with Board of Directors and the Audit Committee to ensure that there is a consistent definition of materiality when reporting errors or omissions.

1.5 The Committee of Sponsoring Organizations (COSO) of the Treadway Commission

Prior to 1940s Internal Auditors were mere clerical positions assisting accountants and verifying figures. Victor Z. Brink (1942) through his treatise on 'Modern Internal Auditing', brought in a total shift from 'control focused' to 'service to management' approach to auditing profession. The final work of Brink and others was to establish the Institution of Internal Auditors (IIA), now a major professional organization, responsible for setting up standards and providing guidance to the profession of Internal Auditing.

Before we explore the work of the Committee of Sponsoring Organisations (COSO), we need to understand who is this committee and what are they sponsoring. COSO is a U.S. private-sector initiative, formed in 1985. COSO is sponsored and funded by five main professional accounting associations and institutes: The American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), The Financial

Executives Institute (FEI), The American Accounting Association (AAA) and the Institute of Management Accountants (IMA). The above organizations were under the aegis of the Securities and Exchange Commission (SEC).

The National Commission on Fraudulent Financial Reporting was formed to study the corporate scandals and the above professional financial organizations sponsored the Commission. Hence the name The Committee of Sponsoring Organisations

Another major transformation took place in the early 90s with the advent of 'Risk Based Auditing' through COSO's initial work on ERM. Notwithstanding, there was however no recognized definition on internal control going through the 80s up until 1992, when the Committee of Sponsoring Organizations (COSO) released 'The COSO Internal Control – Integrated Framework' and established a common definition or understanding for internal controls that has become today's accepted standard. Under SOX, management is now required to report on their internal controls, with the public accounting firm attesting to those internal control reports (Moeller, 2004). All of a sudden the promulgations of COSO on Internal Controls have come alive in 2002 due to SOX implementation.

The Treadway Commission Report

COSO as an organisation, named after its chair, Securities and Exchange Commission (SEC) commissioner James. C. Treadway, the official name as The Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Today, it has become known as just COSO. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

The National Commission on Fraudulent Financial Reporting (commonly known as the Treadway Commission) was also formed in 1985. The Treadway Commission issued its initial report in 1987, and among other items, recommended that the organisations

sponsoring the Commission work together to develop integrated guidance on internal control. As a result of this initial report, the Committee of Sponsoring Organizations (COSO) was formed. The COSO framework involves several key 'concepts' and 'components'.

The COSO Enterprise Risk Management – Integrated Framework

The most important COSO framework which is the topic of interest and basis for building the research in this academic work is now presented.

In the fall of 2004, the Committee of Sponsoring Organizations of the Treadway Commission, known as COSO, released their ENTERPRISE RISK MANAGEMENT—INTEGRATED FRAMEWORK, which was authored by PricewaterhouseCoopers (PwC). This principles-based framework provides direction and criteria for improving an organization's ability to manage risk. Moreover, the enterprise risk management framework is fully aligned with the PwC authored COSO Internal Control—Integrated Framework, which is now used by most organizations as the basis for their reporting under section 404 of Sarbanes Oxley. This enables organizations to build on their investment in internal control as they make improvements in risk management. The COSO ERM is further discussed in Part 1, Section 2.0.

1.6 Standard & Poor's valuation Model

Walker *et al*, (2006) emphasize the importance of rating agencies like Standard & Poor's (S&P) that has already started to incorporate a company's ERM practice into the S&P rating of the company. S&P currently applies this rating to both financial institutions and insurers. Its framework for evaluating ERM at banks includes a review of ERM policies, ERM infrastructure, and ERM methodology.

- ERM policies should address risk culture, appetite, and strategy; control and monitoring; and disclosure and awareness.
- ERM infrastructure covers risk technology, operations, and risk training.

- ERM methodology refers to capital allocation, model vetting, and valuation methods.

The framework for evaluating insurers includes an assessment of risk management culture, risk controls, emerging risk management, risk and capital models, and strategic risk management. S&P has stated that the insurer is rated weak, adequate, strong, or excellent. An adequate rating would mean an insurer has 'fully functioning risk control systems in place for all major risks.'

1.7 Conclusion: *Key Drivers and Trends in ERM*

Lam (2006), Lam et al (2002), Lam (2003), Walker et al, (2006), Wysochi (2000), Berinato (2004) acknowledge that, in the aftermath of notable corporate disasters, board members and executives realize that the only alternative was an effective risk management. More than ever, board members and corporate executives realize the consequences of ineffective risk management.

In response to these events, regulators such as the SEC and the Federal Reserve have increased their examination and enforcement standards. SOX requires enterprise-wide documentation and testing of controls over financial reporting. Furthermore, amendments to the NYSE listing standards require audit committees to discuss risk monitoring and control activities with internal and external auditors. Comparably, Basel II and Solvency II will establish a direct linkage between minimum regulatory capital and the underlying credit risk, market risk, and operational risk exposures of banks and insurance companies, respectively. We have seen in earlier sections that a number of industry initiatives have been organized around the world to establish frameworks and standards for corporate governance and risk management. All these frameworks incorporate corporate governance and internal controls as part of an overall ERM structure. These industry initiatives have clearly established the role of the Board of Directors and Senior Management in risk management.

Companies have also reported significant benefits from their ERM programs, including stock price improvement, debt-rating upgrades, early warning of risks, loss reduction, and

regulatory capital relief. Many companies have even reported that there is an opportunity to convert the ***compliance cost*** into a ***business benefit*** by implementing an ERM program.

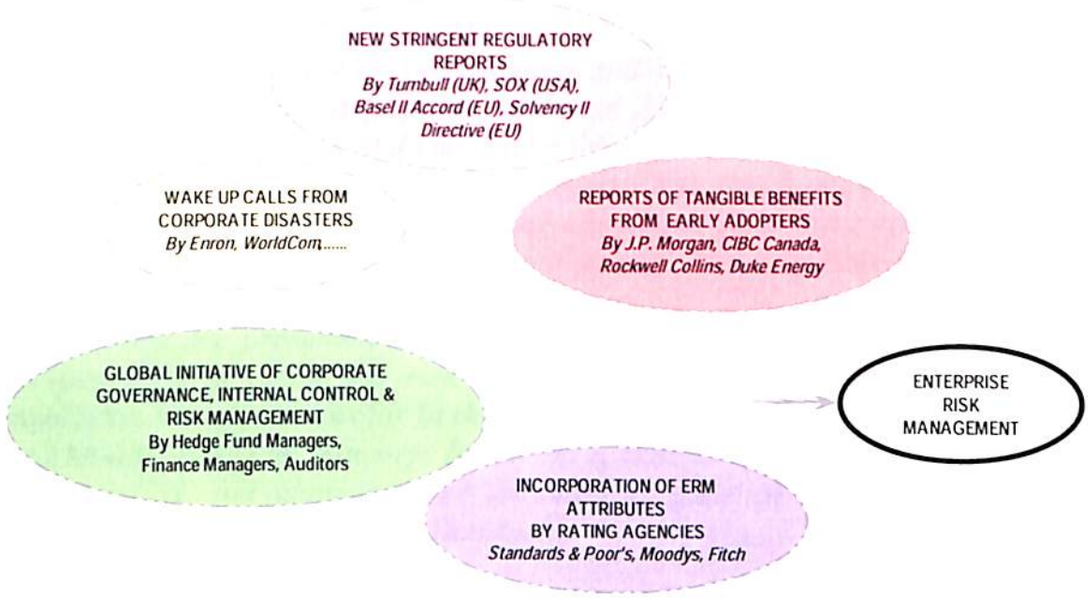

Fig. 1.2 Key Drivers & Trends in Enterprise Risk Management (Source: Adopted from various articles)

In the new business environment, there are clear incentives for best-practice risk management, and based on these various reports, key forces driving the growth in, and acceptance of, ERM has been summarized in Figure 1.3. As stated earlier, a variety of ERM frameworks exist in the industry, nevertheless they propound similar concept through different approaches. Alan Greenspan (2004), emphasizes the importance of risk management and states that, 'better risk management may be the only truly necessary element of success.' The practice of risk management has shifted in a fundamental way and the most commonly used starting point for implementing an ERM initiative is the COSO ERM framework (GARP). The level of interest in risk management has never been greater among corporate executives, financial analysts, and regulators. While it has long been recognized as a core competence in banking, risk management has gained recognition as a critical management discipline in other risk-intensive industries, including securities brokerage, asset management, insurance, ***energy***, and large multinational corporations. The interest in risk management extends all the way to the Corporate Boardroom (Lam, 2006).

----------END OF CHAPTER-1----------