Risk Advisor

February-2017

Risk e (scape) and Control Mechanism

B.K. KHARE & CO.

CHARTERED ACCOUNTANTS

706-708, Sharda Chambers,
New Marine Lines, Mumbai 400 020
Telephone: +91-22 2200 0607 / 7318 / 6360, 6631 5835 / 5836

Mumbai | Pune | Bengaluru | Delhi

INTRODUCTION

Oxford Dictionary defines the term 'Risk' as *a chance or possibility of danger ,loss , injury or other adverse consequences*. This clearly indicates the term is associated with negativity impact to bring down the Organization from the present level. Cloud of uncertainty is the concern for a corporate life in fulfilling set out goals. With respect to an 'unbiased coin', the chance of turning 'Head (Observe)' or 'Tail (Reverse)' is equal, similar as to 'success (**achievement of objectives**)' and 'failure (**non- achievement of objectives)**'. In this background, the word 'Risk' is of phenomenal importance, which connotes as follows.

- ***Risk* is the possibility that an event will occur and adversely affect the achievement of objectives**

- **Events that may have a positive impact represent natural offsets or *opportunities***

The profession of internal audit is fundamentally concerned with evaluating an organisation's **management of risk**. Risk Management and Internal Control are two sides of the same coin, as risk management focuses on the identification of threats and opportunities, and controls are designed to effectively counter threats and take advantage of opportunities. Successful organizations seek to integrate risk management and internal control into all activities, through a framework of risk identification, risk assessment and risk response.

Regulatory Requirements mandating documentation of internal Controls

On the background of corporate financial scandals, notably Enron, WorldCom, etc. the US government took action to improve corporate accountability and governance. Passage of Sarbanes-Oxley Act, 2002 was a fall out of the same. Section 404 of the said Act, which deals with **Management Assessment of Internal Controls**, has the biggest impact on Public companies.

Section 404 requires managements to ensure that they have a comprehensive system of internal controls which enables them to consistently **report complete and accurate financial information for all of their key business transactions.** It also specifies - internal process controls, as well as the system controls over transaction processing; must be in place to ensure the accuracy and completeness of the financial information being reported. These controls should be designed in such a way that they address the potential risks associated with the recording of key business transactions. One of the most important aspects of SOX compliance is that companies must keep their own records concerning their internal control structure. The underlying principle why risk control documentation became essential is that **"internal controls do not exist unless they are documented".**

Being an aspirant to play crucial role in global economy; the Companies Act 2013 and the Amendment Bill 2016 has been enacted with a view to betterment of governance over corporate India and stipulated reporting requirement to make the same effective.

The Reporting requirements at a glance
Section 134 (3) of the Companies Act 2013 provides that 'Board Reports' to include a Director's Responsibility Statement. For the listed entities, the said statement indicates that directors had laid down internal financial controls in place and the same are adequate and working effectively. It also emphasizes 'risk exposure' are within the acceptable limit decided by the board.
Section 177 of the Act stipulates the terms of reference of the Audit Committee shall include 'evaluation of internal financial controls and risk management system'. ***The Act uses the term internal financial controls in the same sense as internal control.***
Clause 17(8) of the SEBI (Listing Agreement and Disclosure Requirements) Regulations 2015 requires that the CEO (Chief Executive Officer) and CFO (Chief Financial Officer) shall submit a certificate to the Board of Directors that they accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of the system.

As transpires from the above, responsibility of the board and audit committee is to establish, maintain and operate effectively an internal control system to ensure effectiveness and adequacy as well the 'business risks' are within acceptable level of the enterprise.

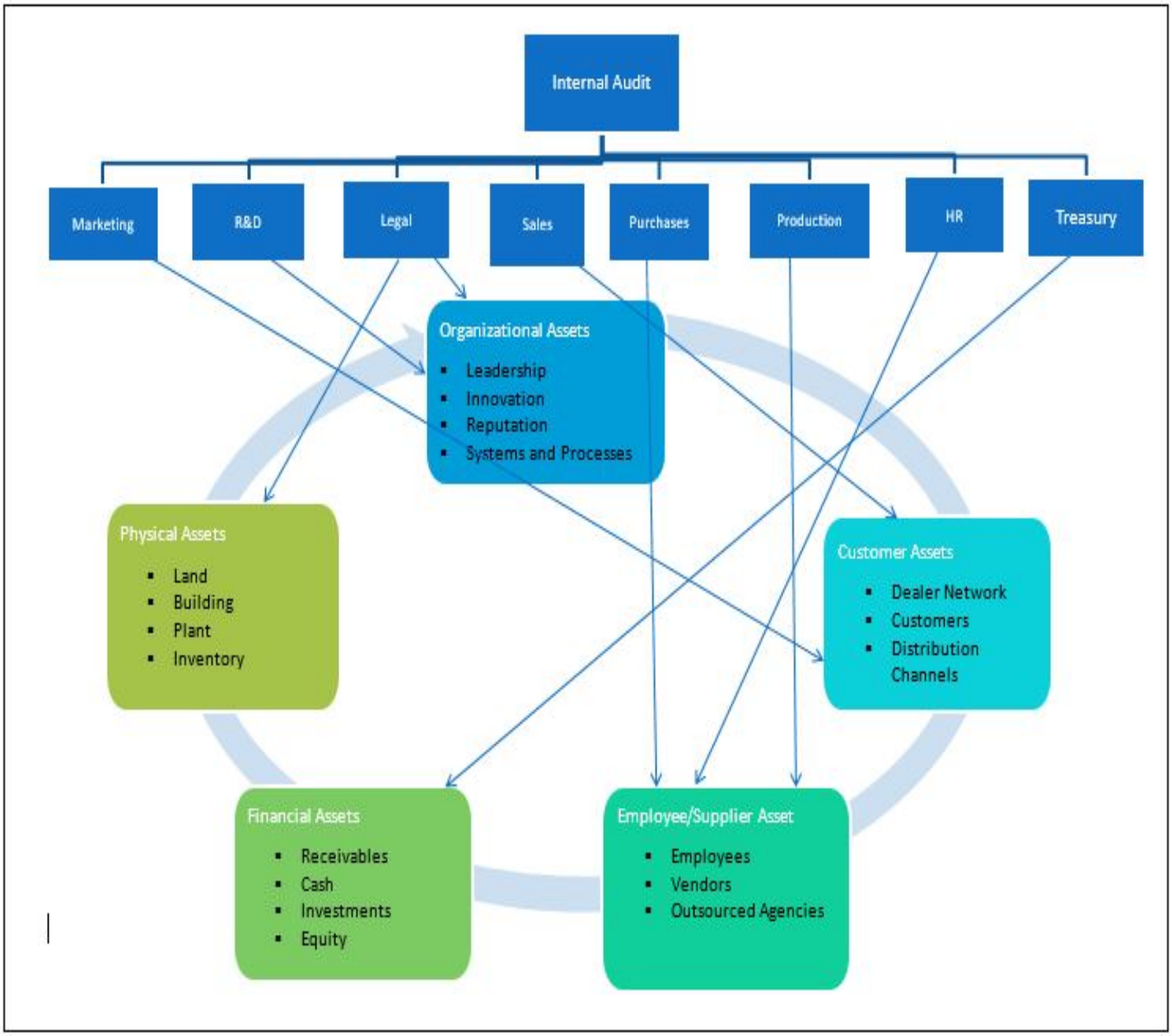
Portfolio View of 'Risk'

An entity consists of various functions/Units (silos) and each one works towards a common organizational goal/objective. Such silos within the Organization having different nature and level of risk, at times having diametrically opposite impacts and hence control mechanism. For example, a Company engaged in export and import handled by two separate silos viz. Sales and Purchases or Units (I- Imports and II –Exports); faces such a situation with respect to rising Dollar against Rupee.

Portfolio view can be obtained by focusing on major risks and organizational objectives to accomplish the same. Let's take an example of a Manufacturing Company, which considers portfolio view of risk in the backdrop of 'Operational Earnings and Excellence' perspective.

The concept of 'portfolio view of risk' introduced here as differentiator between 'Risk Register (RR) 'and 'Risk Control Matrix (RCM) '. In RCM, controls are tested for each of the silo referred hereunder, while RR captures major risks pertaining to one or more of the 'Asset Class' - constituent of the Portfolio. The alignment between the two also indicated hereunder.

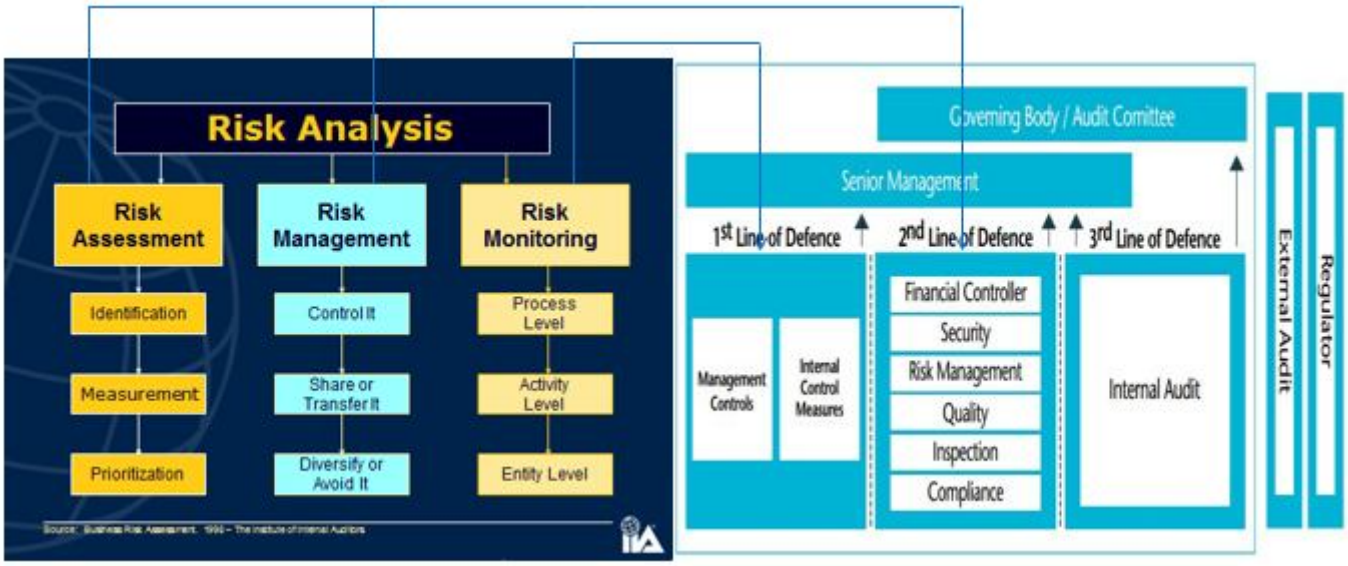
Unlike an 'Investor Portfolio' of securities representing different category (e.g. FMCG, NBFC, Textile etc.) value and volume of investment in different Company Shares and Debentures, the entity risk portfolio consists of different category of Assets like Customer, Employee/Vendor, Financial and Physical forms. Each such category of assets again subdivided into qualitative aspect-wise i.e. Leadership ability/quality, reputation /Brand Equity, germination of Innovative ideas and business model etc. under 'Corporate Assets' category. The 'silos' are attached with each such 'Asset 'category viz. function or department for risk associated with each functional activity. Based on Portfolio of Assets under an Organization, Department (Silos) are attached for identification and mitigation of risk to protect and increase in 'portfolio value'. Even some function having multiple responsibilities attached with asset class of the Organization. The below referred diagrammatic presentation will make the same easier for understanding.


Internal Audit
Marketing
R&D
Legal
Sales
Purchases
Production
HR
Treasury
Organizational Assets
Leadership
Innovation
Reputation
Systems and Processes
Physical Assets
Land
Building
Plant
Inventory
Customer Assets
Dealer Network
Customers
Distribution Channels
Financial Assets
Receivables
Cash
Investments
Equity
Employee/Supplier Asset
Employees
Vendors
Outsourced Agencies

The risk portfolio mechanism is institutionalized through Risk Register and Risk Control Matrices(RCM) , where an internal control mechanism acts as 'sounding board' for identification of granular view through RCM and selection of a focused 'risk basket' in 'Risk Register'.

Risk Register and Risk Control Matrix

The IIA (Institute of Internal Auditors) suggests risk analysis typically under three broad heads viz. Risk Assessment, Risk Management and Risk Monitoring. Under 'Risk Management' activity; Assessment and Monitoring tools are Risk Register (Risk Assessment) and Risk Control Matrices (Risk Monitoring).



The Line of Defence entrusted with responsibilities, which can be leveraged through the tools of Risk Register and Risk Control Matrices (RCM).

a. 1st LoD : Functions that own and manage risk (Risk Monitoring);
b. 2nd LoD : Functions that oversee or specialize in risk management ,compliance (Risk Assessment and Management);
c. 3rd LoD: Functions that provide independent assurance, above all Internal Audit.

A Risk Register is a document which systematically lists down the potential risks to the ongoing operations of an organization and mitigation measures to minimize the likely occurrence of threats. The purpose of a Risk Register is to provide a structured approach to Risk Management. It also allows organizations to assign ownership of that risk to individuals within the organization to develop and track mitigation strategies.

The causal part of 'Risk Register' indicates two types of risk for the entity viz. 'External Risk' and 'Internal Risk'. An example will bring more clarity on the subject.

"BREXIT"…. a highly publicized, followed, reacted upon event of recent times! The decision of people of Great Britain (UK) in favour of leaving European Union (EU) rocked the whole world. The markets across the globe turned volatile, British Pound (GBP) got re-rated, and credit ratings of Britain and European Union were slashed and so on. This event is bound to affect several organizations world over in terms of business volumes, input costs, cost of capital, capacity to raise capital etc. The 'political scenario' of Britain undergone a change, the Prime Minister resigned and new cabinet being formed.

For the Corporates across the globe this event opened new challenges and opportunities, by entering into new geographies and threat by way of currency volatility in countries of European Union. In Indian context, India's exports to UK for 2015-16 were USD 8,829.29 million, whereas Imports were USD 5,193.61 million. With devaluation of GBP, the exports from India might be affected adversely, while imports may rise as they become cheaper.

External Factors:

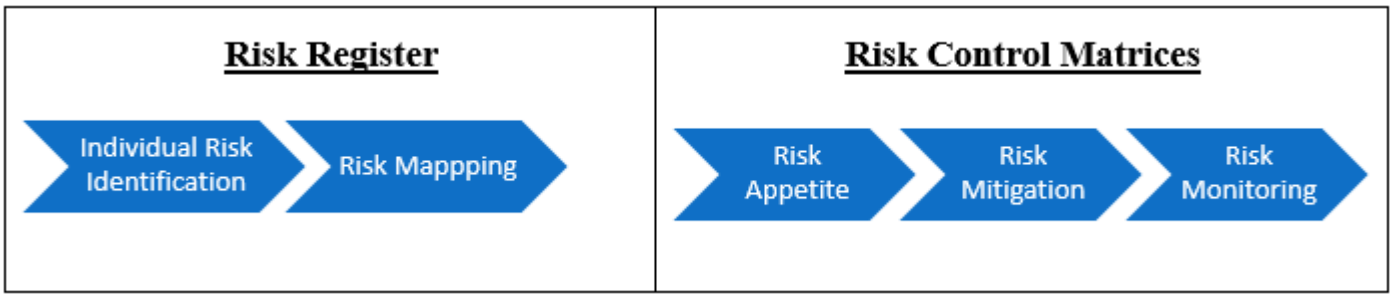
- Economic changes
- Political scenario
- Technological Development of the Industry
- Change in Customer need and expectations
- New Regulations

Internal Factors:

- Corporate restructuring
- Revamped IT System
- New product lines
- New Management structure
- Export Business

Benefits of Risk Register –

- Risk Register provides a systematic approach to Management of Risk.
- A meticulous and continuous updation of the register will enable an organization to avoid unpleasant surprises.
- Tracking of risk events and corrective actions is facilitated for the top management for better control.
- It enables management to evaluate the Risk Impact, Cost of Mitigation and strike balance between the two.



Risk Control Matrix (RCM)

RCM is a matrix that describes the relations among risks and methodologies to control each risk (counter measures to deal with each risk) and is deeply related to factors of internal controls. An RCM provides an overview of different control objectives that organizations should take into consideration and the corresponding controls to safeguard the company against risks which may arise. Once customized to an organization, this document can help the user in assessing each control. The control assessment can then also be summarized to develop an action plan. RCMs assume immense importance in review, documentation and testing of internal controls, whether by management or by auditors.

Comparison between the two

- Risk Register and Risk Control Matrix are interdependent yet mutually exclusive in many ways.

- Risk Register is of wider perspective. It deals with all risks affecting an organization whether emanating from internal factors or external. It focusses on listing down all risks whether or not emanating from internal control failures. Risks emerging from external factors may not form part of an RCM.

  While both tools are mutually exclusive to some extent, they are also complementary e.g. process level controls forming part of Risk Register for monitoring also considered in RCM for micro management. Risk "incorrect and non-timely recording of material issue at Construction Site resulting in inaccurate inventory valuation". RCM on Stores

control will list down the process level controls like maintaining serially controlled issue slips, obtaining acknowledgement of receiver, entering slips into accounting system on daily basis, monthly stock verification by site accountant etc. forming part of Process level control for mitigating the Risk.

A lot of information is captured in typical 'Risk Register'. Our basic idea is to strip back to just risks and controls, emphasizing the controls more than the risks (reversing the norm). As evident from the modified document structure that one 'Control' applies to multiple risks. However, each individual Control to ensure "V (Validation) U (Uniqueness) C (Completeness) and A (Accuracy) – VUCA "while capturing of risk as specified in Risk Register.

Original Document:

Risk	Controls
Risk 1	Control 1 Control 2 Control 3
Risk 2	Control 1 Control 4
Risk 3	Control 2 Control 3
Risk 4	Control 4

Modified Document:

Control	Risk 1	Risk 2	Risk 3	Risk 4
1	1	1	0	0
2	1	0	1	0
3	1	0	1	0
4	0	1	0	1

Conclusion – the differentiator

- The Book titled "Risk" having multiple chapters. The first chapter of the Book, 'Risk Basket', where all the 'Risk' associated with the business are being captured. To make the same under regular monitoring process, only top line risks (Entity Level) with larger impact on the business and its strategy are considered for Board level policy formulation/action. **Risk Control Matrices are themselves a control – over the risk management system; hence might be called as a "meta control"**.

- Risk Control Matrices, basically indicates Risk and mitigation through operating controls and possible concern on Fraud emanating out of control lapses (or control non-existing) or deviations. RCM is more granular (activity based) in nature and starts with "Operating level staff/Manager". On the contrary,' Risk Register' is more crisp in nature having greater strategy bias.

- **The purpose of both are also having difference - from Risk Register 'top' guides bottom in organizational hierarchy , while through RCM , 'bottom' gives assurance to 'top' about health status of various processes.** As per COSO Framework, the 'three Line of Defence (LOD)' propagates responsibility assigned to each Line. The 2nd LOD is entrusted with 'Financial Control, Security, Quality, Inspection, Compliance and Risk Management' to "evaluate and communicate deficiencies" on the areas. The 1st LOD is entrusted with 'overall control and measures'. This 'top' and 'bottom' from the perspective of Organizational set-up and Line of Defence specified in COSO framework. Accordingly, Risk Register / RCM issue to be seen from the said perspective. However, ultimate aim of both is to make the business a place of 'risk free zone' and 'compliant'.

***