CONFIDENTIAL
FOR INTERNAL USE ONLY

uti
UTI Infrastructure
Technology And
Services Limited

# RISK MANAGEMENT POLICY
# OF
# UTI ITSL

DECEMBER 2014

# FOREWORD

It gives me a pleasure to present the Risk Management Policy of the Company which is in compliance with the requirement of the Companies Act, 2013.

Risk Management is a key aspect of Corporate Governance and Code of Conduct which aims to improvise the governance practices across the business activities of the Company. I am confident that this Risk Management Policy of the Company will ensure sustainable business growth of the Company with stability to promote a pro-active approach among the Employees in reporting, evaluating and resolving risks associated with the Company's business.

As per the reporting structure of the policy the Head of the Departments (risk owners) will report the risks to Corporate Risk Management Department (CRMD), who in turn will present the risk report to Board Committee and Board.

In order to achieve the key objectives of the Company, this Policy will establish a structure and disciplined approach to Risk Management, in order to guide Employees to take decisions on risk related issues.

We are grateful to Audit Committee, Risk Management Committee of the Board for its unstinting support and guidance at every stage and the Institute of Public Auditors for making this policy framework possible.

**(PUNIT SAXENA)**

Managing Director & CEO

# Table of Contents

| Chapter No | Para No | Contents | Page No |
|---|---|---|---|
| | | **Glossary** –Terms used in Risk Management | 5-7 |
| 1 | | **Introduction-Risk Management Policy** | |
| | 1.1 | Objectives | 8 |
| | 1.2 | Guiding Principles | 8 |
| | 1.3 | Policy Statement | 9 |
| | 1.4 | Scope and extent of application | 9 |
| 2 | | **What is Risk?** | |
| | 2.1 | Understanding Risk | 10 |
| | 2.2 | Definition | 11 |
| | 2.3 | Part of daily activity of the Company | 11 |
| | 2.4 | Risk or Problem-what is the difference | 12 |
| | 2.5 | Balancing Risk and Control | 13 |
| | 2.6 | Governance in relation to Risk | 14 |
| | 2.7 | Corporate Social Responsibility in relation to Risk | 15 |
| 3 | | **Risk Management Plan** | |
| | 3.1 | The Challenge | 18 |
| | 3.2 | Risk Management as a career path | 18 |
| | 3.3 | Relationship with other processes | 19 |
| | 3.3(i) | Internal Audit | 19 |
| | 3.3(ii) | Business Planning(including Budget) | 20 |
| | 3.3(iii) | Performance Management | 20 |
| | 3.4 | Risk Management Process | 20 |
| | 3.3(a) | Communicate and consultant | 21 |
| | 3.3(a)(i) | External communication and consultation | 21 |
| | 3.3(a)(ii) | Internal communication and consultation | 21 |
| | 3.3(b) | Establish the context | 21 |
| | 3.3(b)(i) | External context | 21 |
| | 3.3(b)(ii) | Internal context | 22 |
| | 3.3(b)(iii) | Risk Management context | 22 |
| | 3.3(c) | Risk Identification | 22 |
| | 3.3(d) | Risk Analysis | 23 |
| | 3.3(e) | Risk Evaluation | 23 |
| | 3.3(e)(1) | Risk impact and probability(Prioritize Risk) | 24 |
| | 3.3(ú)(1)(a) | Probability | 24 |
| | 3.3(ú)(1)(b) | Impact | 24 |
| | 3.3(e)(1)(c) | Impact and Probability chart | 25 |
| | 3.3(f) | Risk Evaluation | 26 |
| | 3.3(g) | Risk Treatment | 26 |
| | 3.3(h) | Monitoring and Review | 26 |
| **4.** | | **Risk Matrix** | 28-46 |

| | | | |
|---|---|---|---|
| **5.** | | **Structure and Administration of Risk Management** | |
| | 5.1 | Need | 47 |
| | 5.2 | Structure | 47 |
| | 5.2(i) | Role of Board of Directors | 48 |
| | 5.2(ii) | Risk Committee of Board | 48 |
| | 5.2(iii) | Corporate Risk Management Department(CRMD) | 50 |
| | 5.2(iii)(a) | Why a separate set up? | 50 |
| | 5.2(iii)(b) | Composition | 50 |
| | 5.2(iii)(c) | Responsibilities | 50 |
| | 5.2(iv) | Risk Owners | 51 |
| | 5.2(iv)(a) | Need | 51 |
| | 5.2(iv)(b) | Set up | 52 |
| | 5.2(iv)(c) | Responsibilities | 52 |
| **6.** | | **Risk Management Tool** | |
| | 6.1 | Introduction | 54 |
| | 6.2 | Management Tools | 54 |
| | 6.2(A) | Risk Register | 54 |
| | 6.2(A)(i) | Need | 55 |
| | 6.2(A)(ii) | Risk Register Template | 56 |
| | 6.2(A)(iii) | Compiling a Risk Register | 56 |
| | 6.2(B) | Risk Management Information System(MIS) | 57 |
| | 6.2(C) | Check List | 59 |
| **7.** | | **Internal Audit in relation to Risk Management** | |
| | 7.1 | Introduction | 65 |
| | 7.2 | Role in Risk Management | 65 |
| | 7.2(a) | Providing Assurance | 66 |
| | 7.2(b) | Consulting Roles | 66 |
| | 7.3 | Safeguards | 67 |
| | 7.4 | Audit Guidelines | 68 |
| | 7.4(A) | In relation to Internal Control | 68 |
| | 7.4(B). | In relation to Risk Management System | 68 |
| | 7.4(C) | In relation to Risk Owners(Heads of Departments) | 69 |
| | 7.4(D). | In relation to Corporate Risk Management Department | 70 |
| | 7.5 | Internal Audit Reporting | 70 |
| | 7.6 | Good Practice checklist for assessing Risk Management | 71 |
| **8.** | | **Periodicity of Review of Risk** | |
| | 8.1 | Introduction | 77 |
| | 8.2 | Periodicity | 77 |

# Glossary

| Term | Explanation |
|---|---|
| **Almost certain** | Expected to occur in most circumstances. In probability terms this may mean that it has greater than 80% probability of occurring. Alternatively this may mean that the event may occur one or more times in a period of up to 5 years |
| **Consequence:** | The outcome of an event expressed either qualitatively or Quantitatively, being a loss, disadvantage or gain. There may be a range of possible outcomes associated with an event |
| **Control:** | A mechanism, process, procedure, system that is used to ensure the positive attributes of an opportunity or mitigate the negative impacts of an identified risk |
| **Corporate Governance** | The manner in which agencies are directed and controlled and held accountable for the achievement of strategic goals and objectives and the delivery of cost-effective services |
| **Eliminating Risk** | An ideal or vision similar to perfect risk controls. In reality this is not achievable |
| **Embedding risk management** | Ensuring that the risk management strategy is reflected in the objectives and function of every level of the organization |
| **Enterprise Risk Management** | A process, effected by an organization board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the organization, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives |
| **Extreme Risk** | This risk requires immediate action and is the responsibility of the CEO or the Executive for their attention |
| **High Risk** | This risk requires action as a priority and responsibility is assigned to the Heads of the Departments for their attention |
| **Impact:** | The positive or negative *consequences* of decisions, events or processes in relation to the achievement of organizational *objective* |
| **Inherent Risk** | The risks of an activity without taking into account existing systems and procedures to control or proposed changes to manage |
| **Integrated Risk Management System** | A risk management system that has been implemented within an organizationȏs business management systems that enables the systematic and coordinated application of a consistent risk management process in all activities undertaken at all levels of the organization. |
| **Likely:** | Will probably occur in most circumstances. In probability terms this may mean that it has between a 60% to 79% probability of occurring. Alternatively this may mean that the event may occur in a period of 5 to 9years. |
| **Likelihood** | The probability or frequency of an event occurring |
| **Low Risk:** | This risk requires a routine response and responsibility is assigned to a nominated officer for their attention |

| | |
|---|---|
| **Mitigate:** | The acts or efforts to reduce the consequences of an event. These may be implemented before, during or after an event. |
| **Moderate Risk** | This risk requires action to be scheduled and monitored |
| **Operational Risk Management** | The oversight of many forms of day-to-day operational risk including the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk does not include market risk or credit risk |
| **Opportunity:** | They are favorable events, which are designed to derive benefits, and have the potential to have a positive influence on the achievement of an organizationῷs objectives. |
| **Possible:** | Might occur at some time. In probability terms this may mean that it has between 40% to 59% probability of occurring. Alternatively this may mean that the event may occur once in a period of 10 to14 years |
| **Rare:** | May occur in exceptional circumstances. In probability terms, may mean that it has less than a 20% probability of occurring. Alternatively this may mean that the event may occur once in 20 or more years. |
| **Residual Risk:** | The remaining *level of risk* after treatment measures have been taken |
| **Risk:** | Risk is the chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood. Note: this means it is a threat that can potentially prevent the organization from meeting its objectives. This includes failing to maximize any opportunity that would help the organization meet its objectives. |
| **Risk Acceptance** | An informed decision to accept the probability and consequences of a particular risk. |
| **Risk Analysis:** | A systematic use of available information to determine how often a specified event may occur and the magnitude of its consequences. It is used to establish a level of risk |
| **Risk Assessment** | The collective term for the processes of risk identification, risk analysis and risk evaluation |
| **Risk Avoidance** | An informed decision not to proceed with the activity likely to create risk. Risk avoidance may increase the significance of other risks or may lead to the loss of opportunities for gain |
| **Risk Control** | That part of risk management which involves the implementation of policies, standards, procedures, internal controls and physical changes to eliminate minimize or manage the negative consequences of risks. Risk controls are primarily applied to risk sources |
| **Risk or Opportunities categories:** | The categories used by the organization to group similar opportunities or risks for the purposes of reporting and assigning responsibility. These include Strategic, Operational, Financial, Reputation and Legal/Regulatory/Compliance. |
| **Risk Evaluation** | The process used to determine risk management priorities<br>by comparing the level of risk against predetermined standards, target risk level or other criteria |
| **Risk Identification** | A systematic process applied to the organizationῷs objectives and activities to identify possible *risk sources* and causes and |

| | |
|---|---|
| | potential consequences or impacts should a risk occur. |
| **Risk owner** | The person occupying a position that has a delegated authority and accountability to make a decision to do or not to do something about a specific risk |
| **Risk Management** | The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects in order to achieve organizational objectives |
| **Risk Rating** | The combination of the consequence and likelihood with reference to the Risk Assessment Criteria Matrix. The Risk rating is assessed as either low, moderate, high or extreme |
| **Risk Register** | A complete list of risks identified by the management which threaten the objectives and processes of the organization. |
| **Risk sources** | The underlying reasons or events that may trigger or contribute to a risk occurring in an organization |
| **Risk Treatment** | The selection and implementation of appropriate options for dealing with risk |
| **Risk Transfer** | Transferring the risk to another party in whole or in part through legislative compliance, contract, insurance or other means |
| **Strategic Risk Management** | A strategic approach to risk management depends on identifying risks against key organizational objectives, which supports the strategic planning, and development processes of an organization |
| **Treatment** | The application of a course of action to either enhance or exploit an opportunity or to reduce the likelihood or consequence of a risk |

# CHAPTER 1

## INTRODUCTION TO RISK MANAGEMENT POLICY

### 1.1 OBJECTIVES

The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Matrix, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are to:

i. ensure that all the current and future risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed;

ii. establish a framework for the companyồs risk management process and to ensure companywide implementation;

iii. enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices;

iv. assure business growth with financial stability.

### 1.2 GUIDING PRINCIPLES

In order to fulfill the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:

i. All business decisions will be made with the prior information and acceptance of risk involved.

ii. The Risk Management Policy shall provide for the enhancement and protection of business value from uncertainties and consequent losses.

iii. All employees of the company shall be made aware of risks in their respective domains and their mitigation measures.

iv. The risk mitigation measures adopted by the company shall be effective in the long-term and to the extent possible be embedded in the business processes of the company.

v. Risk tolerance levels will be regularly reviewed and decided upon depending on the change in companyôs strategy.

vi. The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

## 1.3 POLICY STATEMENT

The policy statement is as given below:

A. To ensure protection of shareholder value through the establishment of an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks

B. To provide clear and strong basis for informed decision making at all levels of the organization

C. To continually strive towards strengthening the Risk Management System through continuous learning and improvement

## 1.4 SCOPE AND EXTENT OF APPLICATION

The policy guidelines are devised in the context of the future growth objectives, business profile envisaged and new business endeavors including new products and services that may be necessary to achieve these goals and the emerging global standards and best practices amongst comparable organizations. This policy is meant to ensure continuity of business and protection of interests of the investors and thus covers all the activities within the company and events outside the company which have a bearing on the companyôs business. The policy shall operate in conjunction with other business and operating/administrative policies.

.

# CHAPTER 2

## WHAT IS RISK?

***Risk is the likely shortfall between the desired levels of performance and actual performance at future time***

### 2.1 UNDERSTANDING RISK

The globalization of business, growing complexity of transaction and new age IT infrastructure have revolutionized the concept of trade and commerce. However parallel to the great upsurge another growing factor has been haunting corporate board rooms-that is the phenomenon of **Risk**. This is an all pervading term covering operational, financial and regulatory domains.

In most cases we observe that there is deviation in what we achieve from what we had planned or what we had expected. The unpredictability of future is due to uncertainties associated with the steps that we undertake in the process or various factors that influence the processes that are necessary to achieve our planned objective.

Let us understand it through an example.

Say we have to keep an appointment that is very important and we to reach there in time. In order to keep an appointment one has to get ready in time, arrange a transport and travel to the distance to the place of appointment. All these factors are inseparable associated with the process of reaching the place of appointment. There are uncertainties associated with all of them. One may get ready early or be delayed, transport may become available well in time or there may be difficulty and delay in getting it, there may be traffic jam or traffic disorder or traffic flow may be very smooth or vehicle may break down on  the way or it may be trouble free drive. If everything goes well one would reach well in time. These uncertainties may also become instrumental in oneȏs failing to reach in time. In other words there is a risk of reaching late for the appointment, which is due to uncertainties associated with the factors mentioned above. These factors are the risk elements or contributors to the uncertainties. Risk would arise when these uncertainties affect adversely.

## 2.2 Definition

Risk is the ñeffect of uncertainty on objectivesò and an effect is a positive or negative deviation from what is expected. So, risk is the chance that there will be a positive or negative deviation from the objective you expect to achieve

A business risk is the threat that an event or action will adversely affect an organizationôs ability to maximize stakeholder value and to achieve its business objectives.

Every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for the management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity with potential to erode or enhance value.

Risk in itself is not bad, risk is essential to progress, and failure is often a key part of learning. But there is need to balance the possible negative consequences of risk against the potential benefits of its associated opportunity. Organization take risk for the reasons indicated below:

I. Additional distribution channels.

II. Increase or maintain customer base.

III. Improve customer relationship through service offering.

IV. Customer demand

## 2.3 Part of daily activities of the Company

Risk is a part of daily activities of everyone in the organization as indicated below:-

**(i). Focus on personal accountability**: Spell out the responsibility, activity and accountability of every employee in the organization.

**(ii). Hold your business accountable:** Get the Heads of Departments to assess the maturity of their risk processes, rectify any flaws and sign off on the risk they assumed.

**(iii). Lead from the front:** Show your Heads of Departments that you are serious about risk management by regularly reviewing key risks, reviewing those manage risk well and punishing those who do not.

**(iv). Refocus risk management function:** Reposition your risk management function to do the job it is supposed to be doing i.e. providing information, advice and assurance.

## 2.4 Risks or Problems – What's the Difference?

A risk is an uncertain future event that could have a negative effect (threat) or a positive effect (opportunity) on the project objectives. But a problem statement describes a 100% certain condition that exists now and threatens achieving the project objectives. Understanding the difference between a risk (threat) and a problem is important because they are treated differently in planning and execution.

A problem statement would be: **"We have insufficient resources to conduct the beta tests which will delay the project by one week."**

A risk statement could be: **"We may have insufficient resources to conduct the beta tests which would delay the project by one week."**

These two statements are very similar but have significantly different meanings in planning and executing the project.

The first statement is a problem statement and implies almost 100% certainty (very few events have 100% certainty). The project plan must deal with this real problem on its face value. The project plan must specify how this issue will be resolved before the project plan can be approved.

The second statement is a risk statement with an implied probability (may have) and estimated impact to the project if the risk event occurs.

Once we have identified the risk, a qualitative analysis is performed to assess the risk consequence or risk score which is used to prioritize the risk relative to other identified project risks. If the risk event turns out to have a relatively high consequence, a quantitative expected value analysis may be performed to estimate the probability of the risk and the expected value impact on the project objectives in terms of scope, cost and schedule.

A risk response plan should be developed to mitigate or eliminate the risk consequence. Typically, money, time and other resources will be allocated up front in the project plan to mitigate the high level risk before it occurs. After mitigation, any residual risk consequence remaining must be estimated.

## 2.5. Balancing Risk and Control

Risk is the probability that an event or action will adversely affect the organization. The primary categories of risk are errors, omissions, delay and fraud. In order to achieve goals and objectives, management needs to effectively balance risks and controls. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk. By performing this balancing act "reasonable assuranceò can be attained. As it relates to financial and compliance goals, being out of balance can cause the following problems:

| **Excessive Risks** | **Excessive Controls** |
|---|---|
| Loss of Assets, Donor or Grants | Increased Bureaucracy |
| Poor Business Decisions | Reduced Productivity |
| Noncompliance | Increased Complexity |
| Increased Regulations | Increased Cycle Time |
| Public Scandals | Increase in no value activities |

In order to achieve a balance between risk and controls**, internal controls should be proactive, value-added, and cost-effective and address exposure to risks.**

### 2.6. Governance in relation to Risk

Governance is essentially a guidance system aimed at achieving objectives *i.e.* it is objectives-focused. Risk management is an essential element and the following statements outline the relationship between risk, control, strategies and governance ð

a. An organization is a group of people working together to achieve objectives and is multi-layered.

b. Objectives are the results or goals set by the organization and are also multilayered with alignment of objectives and organizational layers.

c. Risk management develops risk treatment plans that are at the same time the controls and strategies associated with each objective.

d. Risk management is therefore part of each objective at all levels of the organization and is also multilayered by this alignment to objectives.

e. By associating the management of risk with objectives at all levels of the organization it becomes fully integrated as an enterprise-wide system.

f. Risk management develops the control environment and provides reasonable assurance that objectives will be reached within an acceptable degree of residual risk. This is governance.

In essence ð

1. The purpose or focus of the organization is defined by its corporate objectives and by their translation into operational objectives throughout the organization. In short, strategies and controls = objectives + risk management.

2. Reporting against performance measures for each objective is also a report on the effectiveness of strategies, controls and the risk management process for that objective. Performance reporting therefore provides a continuous risk management reporting platform.
3. Risk management not only provides a strategy for treating risks that might prevent an organization from achieving its objectives, but also provides the flexibility for the organization to respond to unexpected threats and take advantage of opportunities.

Risk management, therefore, is dynamic in that it provides organizational resilience as well as control and provides competitive advantage.

## 2.7. Corporate Social Responsibility (CSR) in relation to Risk

CSR has received a lot of attention particularly from firms who have encountered reputational challenges to their brand. While CSR is quickly becoming an integral part of some companiesô business strategy and corporate governance framework, others feel that CSR is not part of their business mandate of creating profits for the business and its shareholders? It is never simple to demonstrate the business case for CSR, but those companies who have adopted CSR policies and programs have done so on the grounds that it is a good business proposition. For many companies, investing in CSR policies and programs is a way to manage a companyôs reputational risk, manage relationships between the company and shareholders and other stakeholders, and preempt potential problems in how products are produced, sourced and sold.

CSR is still a controversial and somewhat amorphous area that many businesses and management either reject as bad business practices, or do not fully understand what CSR is and how it can be implemented. Many businesses still have the following questions:

a) What exactly is CSR and what policies and practices can be implemented and how?
b) Is CSR a costly strategy?

c) How have firms implemented CSR policies and what are the successes and benefits

For the firms that have embraced CSR, they view it is an important part of their business strategy. They recognize that it requires human and financial resources to create and implement, but they believe that it is a good business proposition and good business value. For some businesses, developing CSR policies and programs is not only about good business strategy, but also about ensuring that the communities where the company produces or sells it products or services are well-served by the company. These companies view the relationship with their communities, producers and consumers as symbiotic and mutually beneficial. Furthermore, many companies view CSR as good corporate governance as it allows companies to better engage with many of their stakeholders, including investors and consumers.

These rationales have motivated companies to develop various types of CSR strategies, policies and program. CSR takes many different forms and can be rationalized in many different ways by companies whether engaged in local or global business enterprises. Some examples of CSR policies include a corporate policy on CSR, policies on human rights, policies on sourcing and suppliers to ensure that the supply chain functions according to the companyõs overall CSR policy, investments in communities such as schools and infrastructure, health and safety policies for the goods and services that the company sells to ensure that the business process does not create environmental or health ñexternalitiesò.

These policies require the allocation of human and financial resources. Even more difficult can be to integrate and infuse the CSR policies and commitments into the cultural identity of the company. Despite these challenges, many companies around the world have made these investments and have argued that it is good business strategy and a necessary part of their corporate governance framework. Even if companies and their management are not convinced on the merits of CSR as a business strategy and integral practice of good corporate governance, companies should remain open to further considering and evaluating the importance and benefits of CSR. More and more academic studies and company case studies are illustrating that these CSR policies bring significant benefits for the company, and assist it in managing reputational risk, improving relationships with stakeholders and improving the companyƗs corporate governance procedures.

# CHAPTER 3

## Risk Management Plan

## A good risk management foster vigilance in times of calm and instills discipline in times of crisis

### 1. The Challenge

Risk management is not as well developed as are some of the more traditional project management disciplines. Some organizations feel that risk management is too specialized or advanced for them. Others believe that risk management is optional. Others fear that risk management may expose flaws in their companyộs plans and strategies that will hurt them in the competitive market. Certainly these organizations will not talk openly and honestly about risk and will ñshoot the messengerò that brings risk to their attention

From an organizational standpoint, the traditional approach to managing the various risks to which the organization is exposed was to treat them separately, appointing someone to manage each risk. Managing a particular kind of risk became the job of individual specialists. Doing that job well meant focusing exclusively on "their" particular kind of risk.

Organizations have long tolerated this segmented approach to risk management, but have never been really satisfied with it since it ignores the interdependence of many risks. It erects barriers to exploiting natural hedges among the risks and sub-optimizes the treatment of total risk.

They've known that if it were possible to address all risks on a consistent basis, they would improve the efficient use of their capital. They would also make better strategic decisions, and be better informed about taking on risks to create value.

### 2. Risk Management as a Career Path

Risk management is a central part of **any** organizationộs strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. Risks are continuously changing along with the environment around and hence risk management is a continuous and cyclical process. Essential principles to effective risk management are:-

| | |
|---|---|
| **Corporate Perspective** | • Viewing developments within the context of strategic goals.<br>• Recognizing both the potential value of opportunity and the potential impact of adverse effects. |
| **Forward-looking View** | • Thinking towards tomorrow, identifying uncertainties, anticipating potential outcomes.<br>• Managing resources and activities while anticipating uncertainties. |
| **Open Communication** | • Encouraging free-flowing information at and between all levels.<br>• Enabling formal, informal and impromptu communication.<br>• Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk). |
| **Integrated Management** | • Making risk management an integral and vital part of the organization<br>• Adapting risk management methods and tools to a project's infrastructure and culture. |
| **Continuous Process** | • Sustaining constant vigilance.<br>• Identifying and managing risks routinely through all phases of the company's activities. |
| **Shared Vision** | • Mutual vision based on common purpose, shared ownership and collective communication.<br>• Focusing on results. |
| **Teamwork** | • Working co-operatively to achieve common goals.<br>• Pooling talent, skills and knowledge. |

### 3. Relationship with other processes

Risk management is not a stand-alone discipline. In order to maximize risk management benefits and opportunities, it needs to be integrated with existing business processes. Some of the key business processes with which risk alignment is necessary are:

- **Internal Audit** ï Internal Audit reviews the effectiveness of controls. Alignment between the Internal Audit and that of the controls within the Risk Management process is critical, and the role of Corporate Risk Management Department will seek to align these core processes.

- **Business Planning (including budget)** ï Identifying risk during the business planning process helps in setting up realistic delivery timelines for strategies/ activities or to choose to remove a strategy/ activity if the associated risks are too high or unmanageable. The impact of changing risk levels over the year can then be mapped to the relevant objective, enabling us to conduct more timely expectation management with key stakeholders.

- **Performance Management** ï All risk responsibilities, whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership or implementation of risk treatments should be included within the relevant individualsô performance plans.

## Risk Management Process

Key processes in risk management are:-

- Communicate and consult
- Establish the context
- Identify risks
- Analyse risks
- Evaluate risks
- Treat risks
- Monitor and review.

It is important to follow this process when conducting risk management as this ensures that the approach to risk management is both comprehensive and consistent.

This process is formally conducted across the entire organization on an annual basis. This occurs in conjunction with the corporate and business planning process and involves the review and update of risk profiles for the enterprise as a whole includes a review for each individual division. This illustrates a ñtop-downò and aòbottom-upò approach to risk management.

Although this process is conducted across the entire organization on an annual basis, risk management is not solely an annual process. It should be occurring at all times and in relation to all business activities. Therefore everyone has a responsibility to continually apply this process when making business decisions and when conducting day-to-day management.

Each process step is described in detail as under:-

(a). Communicate and Consult

Communication and consultation with internal and external stakeholders is important throughout the risk management process to ensure the organization has a comprehensive picture of the risks it faces.

**(i)** ***External communication and consultation*** is targeted at informing external stakeholders of:

- The organisationôs risk management approach.
- The effectiveness of risk management approach.
- Requesting feedback where appropriate.

**Risk management is key governance and management function, which external stakeholders, including Government and industry, are, paying, increased attention to. Satisfying these stakeholders with appropriate risk management practices will influence their perception of the organisation.**

**(ii)** ***Internal communication and consultation*** is aimed at informing internal stakeholders of:

- The risk management process.
- Seeking feedback in relation to the process.
- Key risks and their responsibilities relating to management of these.

**(b). Establish the Context**

This means considering:

**(i).*External context***

Building an understanding of external stakeholders and hence the extent to which this external environment will impact on companyôs ability to achieve corporate objectives:

- Business, Social, Regulatory, Cultural, Competitive, Financial and Political Environments in which we operate.
- It also involves considering our strengths, weaknesses, opportunities and threats (SWOT).

**(ii).*Internal context***

This is aimed at understanding organizational elements and the way they interact, such as:

- Culture, internal stakeholders, structure, capabilities (in terms of resources such as people, systems, processes and capital), goals and objectives and the strategies in place to achieve these.

**(iii). *Risk management context***

The goals, objectives, strategies, scope and parameters for the risk management process itself must also be considered.

**©. Risk Identification**

After establishing the context, the next step in the process of managing risk is to identify the potential risks. Risk identification is a key step in the risk management process to ensure a complete list of risks is identified.

Risks can be identified using various tools and techniques including:

i. Structured interviews.
ii. Strategic and business plans.
iii. Post event report.
iv. Local and overseas experience.
v. Focus group.
vi. Surveys and questionnaire.
vii. Check list.
viii. Audit Reports

Part of risk identification also involves identifying risks that may arise ñover the horizonò. Some examples of possible considerations could include:

- Worldwide events.
- Rising public expectations re public sector entities.
- Changing public attitudes towards Government.

Identifying all risk elements provides a better understanding of the risk and assists when considering current controls and identifying further treatment actions.

### (d). Risk Analysis

Once a risk is identified, it is important to adequately describe it. The components of a comprehensive risk description are:

- Event e.g. High staff turnover;
- Cause e.g. Staff job dissatisfaction; and
- Impact i.e. Inability to achieve strategic objectives.

Risk analysis involves:

- Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk;
- Assessing the effectiveness of current controls;
- Identifying the likelihood of the risk occurring; and
- Identifying the potential consequence or impact that would result if the risk was to occur.

When evaluating the effectiveness of current controls, the factors to consider include consistency of application, understanding of control content and documentation of controls where appropriate. Controls are aimed at bringing the risk within an acceptable level. The evaluation of current controls can occur through several different processes including:

- Control self-assessment;
- Internal Audit reviewing the effectiveness of controls; and
- External Audit reviewing the effectiveness of controls.

The consequence and likelihood ratings, as identified after consideration of current controls, are combined to determine the overall risk level.

### (e). Risk Evaluation

Risk evaluation involves considering the riskös overall risk level. This allows determination of whether further risk treatment actions are required to bring the risk within a level acceptable. The output of the risk evaluation phase is a prioritized list of risk

### 3.3(e) (1) Risk Impact/Probability (Prioritize Risks)

Risk Management is important function in an organization today. Companies undertake increasingly complex and ambitious projects and these projects must be executed successfully, in an uncertain and often risk environment. Does this mean that the company should try to address each and every risk that it might face? Probably not- in all but the most critical environments, this can be too expensive, both in terms of time and resources. Instead there is a need to prioritize the risks. If this is done effectively, then the majority of time and efforts can be focused on important risks.

The risk impact/probability primarily has two dimensions:

**(a). Probability:** A risk is an event that ómayôoccur. The probability of it occurring can range from just above 0 percent to just 100(it cannot be 100 percent because it would be certainty and it cannot be 0 percent or it would not be risk). Assess the probability of each risk occurring and assign it a rating. For example, one could use the scale of 1 to 10. Assign a score of 1 when the risk is extremely unlikely to occur and use a score of 10 when the risk is extremely likely to occur.

**(b). Impact:** A risk, by its very nature, always has a negative impact. Estimate the impact on the companyôs activities if it occurs. Again do this for each and every risk on the list by using 1-10 scale. Assign it 1 for little impact and a score of 10for a huge, catastrophic impact.

**(c).** The following table gives the impact and probability chart which helps in categorizing the risk- High, Medium, Low, Not applicable, Need information and To be documented:-

| **Category of risk** | **Likelihood of Occurrence (Probability)** | **Risk becomes an issue (Impact)** | **Likely hood of risk materializing (Scale)** |
|---|---|---|---|
| High | Exhibits the high risk, has happened frequently, has very significant chances of occurring in future, event has already happened. | The issue will have major impact on the system and is likely to cause significant disruption in service, a very visible event. | 7-10 |
| Medium | Has happened occasionally or has a reasonable but not completely expected chance of happening in future. | The issue will have some impact on system and be visible to number of users. A probable disruption in service to some non-critical users is expected. | 4-6 |
| Low | Has happened very infrequently or is expected not to happen except infrequently. | No service disruption or negative effects are expected. Any negative impact can be corrected without any significant efforts or visibility. | 1-3 |
| Not applicable | This risk is irrelevant to the goal and operation of the company. | This risk is irrelevant to the goal and operation of the company. | 0 |
| Need Information | Impossible to determine probability with the available information. Information must come from an outside source. Consider high probability unless otherwise identified | Impossible to determine the probability with the current available information. Information must come from outside source. Consider high impact until otherwise identified. | 7-10 |
| To be Documented | Additional study will be required. Consider high probability until otherwise identified. | Study will be required. Consider high impact until otherwise identified | 7-10s |

Notes:

i. If the probability of an event occurring is zero, then it will be removed from consideration. Thereӧs no reason to consider things that simply cannot happen.

ii. If the impact of an event is zero, it should not be listed. Thereӧs no reason to consider things that are irrelevant, regardless of the probability.

iii. There is no universal formula for combining Probability and Impact; that will vary between organization and organization.

**(f). Risk Evaluation**

Risk evaluation involves considering the riskøs overall risk level. This allows determination of whether further risk treatment actions are required to bring the risk within a level acceptable. The output of the risk evaluation phase is a prioritized list of risks.

**(g). Risk Treatment**

Risk treatment is the process of selecting and implementing measures to modify risk. A system of risk treatment should provide as minimum:

- **effective and efficient operation of the Company**: The risk analysis process assists the effective and efficient operation of the company by identifying those risks which require attention by the management.
- **effective internal controls**: The degree to which the risk will either be eliminated or reduced by the proposed control measures.
- **compliance with laws and regulations**: Compliance with laws and regulations is not an option. The company must understand the applicable laws and implement a system to control to achieve compliance.

Possible risk treatment options include:

- **Avoid the risk** ï change business process or objective so as to avoid the risk;
- **Change the likelihood** ï undertake actions aimed at reducing the cause of the risk;
- **Change the consequence** ï undertake actions aimed at reducing the impact of the risk;
- **Share/transfer the risk** ï transfer ownership and liability to a third party; and
- **Retain the risk** ï accept the impact of the risk.

When determining the preferred treatment option, consideration should be given to the cost of the treatment as compared to the likely risk reduction that will result (cost benefit analysis).

**(h). Monitoring and Review**

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policies and standard compliance should be carried out and standards performance reviewed to identify opportunities for improvement. The monitoring process should provide assurance that there are appropriate controls in place and the procedures are understood and followed.

Monitoring and review process determine whether:

- the measures adopted resulted in what was intended,
- the procedures adopted and information gathered for undertaking the assessment were appropriate,
- Improved knowledge would have helped to reach decisions and identify what lessons could be learned for future assessment and management of risks.

The role of the Board of Directors/Audit Committee vis-à-vis the responsibilities of the REC, CRMD and Risk Owners in relation to identification, assessment and treatment of risks are given in **Chapter 4. The Structure and Administration of Risk Management** which may be referred.

.

# CHAPTER 4

## Risk Matrix

| | | | | | | |
|---|---|---|---|---|---|---|
| **Risk Rating:** | 7-10 | 4-6 | 1-3 | 0 | 7-10 | 7-10 |
| **Risk Category:** | High (H), | Medium (M), | Low (L), | Not applicable (NA), | Need information (NI) | To be documented (TBD) |

| Risk | Root Cause | Impact | Risk rating &Category | Mitigating Factor | Responsibility (Risk Owner) |
|---|---|---|---|---|---|
| | | **A. Business Environment and Industry Risks** | | | |
| **Threat to market share** | • Competitor acquiring business through prompt service and offering discounts.<br>• Delayed dispatch of PAN cards.<br>• Delayed response to the communication from applicants.<br>• Absence of second level of verification of applications and agency data.<br>• Untrained staff leading to acceptance of incomplete/incorrect applications.<br>• Delay receipt of applications from Branches / PSAs. | Erosion of revenue and low profitability. | 7-10<br>High | • Vigorous marketing efforts with targets for each marketing staff.<br>• Incentive to marketing staff that excel targets.<br>• The company should have dedicated knowledge management function to provide knowledge of new products, market and trade development and also maintain links to important information sources relevant to the industry.<br>• Organization of PAN camps at frequent intervals.<br>• Strict compliance of timeline for attending to applicantôs communication/queries and dispatch of cards.<br>• Interim response to applicants through computer generated mails.<br>• Add check trail in the system | Vice President Asstt/Dy Vice President,PDC/PPC/Branches |

| | | | | | |
|---|---|---|---|---|---|
| | • Lack of follow up with Branches / PSAs for applications under objections. | | | including data sent to printer, printed cards received and cards actually dispatched<br>• Representation to Government for unethical practices of the competitor.<br>• Validation of applications and agency data by supervisory staff.<br>• Orientation and re-orientation programmes for the counter staff.<br>• Check list for the staff and PSAs receiving applications.<br>• Vigorous follow up with the branches/PSAs for applications under objection. | |
| **Dependence on single client** | • Failure to widen the client base.<br>• Absence of long term marketing strategy.<br>• Danger of a change of government | Inconsistent and low return | 7-10<br>High | • Proactive liaising with Government Departments to maintain healthy relations.<br>• Increase client base through extensive marketing efforts which should strive to broaden its base so as to reduce its vulnerability of dependence on one client.<br>• External perceptions are regularly measured (among investors, media, pressure groups, etc)<br>• Establish relationships and trust with pressure groups and other potential criticsô | Vice President Asstt/Dy Vice President, PAN Division, DOIT/Projects, Insurance/CGHS/ECHS/NABARD etc., Infrastructure Division and Regional Offices |

| | | | | | |
|---|---|---|---|---|---|
| **Reputation Risk (Poor brand perception**). | • Failure to deliver minimum standards of service.<br>• Non<br>• compliance with regulation/legal obligations<br>• Loss of key skills and talent.<br>• Employee fraud.<br>• Loss/theft of intellectual property<br>• Leakage of investorsô financial data.<br>• Payments to ineligible persons due to non-availability of the applications and specimen signatures of the investors.<br>• Absence of the system of cross verification of the duplicate issue of certificates. | • Undermine public trust in companyôs products or brand.<br>• Poor investors satisfaction | 4-6 Medium | • Ensuring effective co-ordination between different functional groups (Divisions and Regional offices).<br>• Controls are systematically enforced.<br>• Develop programme for corporate social responsibility to address possible sources of reputational risk.<br>• Investorsó/applicantsô increased focus on investing/getting services from ethical entities.<br>• Reputational threats are systematically tracked<br>• Protect in- house software developed for various project under copyright laws as it is one of the most tradable properties in the digital market place.<br>• Limit the access to the important and confidential data only to senior officers and also ensuring that it is difficult to get access to sensitive data by other staff.<br>• Cross verification of claims of ineligible investors before issue of duplicate certificates | Vice President Asstt/Dy Vice President PAN Division, Western Region, Insurance/CGHS/ECHS/ NABARD etc., Infrastructure Division and Regional Offices, HR Division, DOIT/Projects |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  |  | (issue public notices) and payments to ineligible persons. |  |
| **B. Strategic Business Risks** |  |  |  |  |  |
| **Operational. Risk** | • Improper/inadequate follow up of the provisions of Service Level Agreement with the Income Tax Department and CGHS.<br>• Appointment of PSAs without proper verification.<br>• Lack of follow up with the applicants for cards returned undelivered.<br>• Lack of synchronization of procedure for destruction of RUD cards by branches and PDC.(Kolkata branch destroys the RUD cards after six months while in PDC the destruction period | Effect on the likelihood of achieving the corporate objectives. | 4-6<br>Medium | • Control mechanism for ensuring compliance of the various provisions of the service level agreements.<br>• Effective implementation of IT System by sending computer generated mails to the applicants for RUD cards and cheques. The system should also record such communications.<br>• Detail comprehensive guidelines and monitoring mechanism for appointment and for appraising performance of PSAs.<br>• Modify SOP for destruction of RUD cards which should be in line with the provision of Service Level Agreement.<br>• Periodical verification of RUD cards and its verification with master.<br>• System should reflect reason wise analysis of pending cases and also time lag in payment of hospital bills.<br>• Periodical reconciliation of the records of System Accounts and DOIT with analysis and reasons for | Vice President Asstt/Dy Vice President, Insurance/CGHS/ECHS/NABARD, PDC Southern Region Infrastructure Division and System Accounts. |

| | | | | | |
|---|---|---|---|---|---|
| | is one year)<br>- Absence of physical verification of RUD cards.<br>- Delayed settlement of hospital bills.<br>- Variation in figures of recoupment received as per the System Accounts and that shown by DOIT.<br>- Non availability /validation with master files of the CGHS beneficiaries<br>- Unique reference for each card instead CGHS card number resulting in multiple claims.<br>- Delay in decision making.<br>- Rejection of valuation by the clients.<br>- Mix up of Companyôs | | | variations. Management Information system need to be introduced as per the requirement of Service Level Agreement<br>- Vigorous follow up with CGHS for making available the beneficiaries data.<br>- Card number is unique number allotted by CGHS and should be the primary key in the system to identify multiple claims.<br>- Modify software to indicate the date of physical receipt of the folders.<br>- Enforce more accountability for delay in decision making leading to financial impact.<br>- Develop an internal monitoring mechanism for approval of files. Identify the key decision points, the delay in which will be detrimental to the overall objectives of the company. The estimated turnaround time for these decisions and the responsibility centers for decision making should be clearly identified.<br>- De-roaster the valuers who are constantly over/under valuing the premises. Link payments to such valuers only on confirmation of | |

| | | | | | |
|---|---|---|---|---|---|
| | valuers with the owners of premises resulting in over/undervaluation. | | | valuation by the Valuation Committee/clients. | |
| **C. .Human Resource Risks** | | | | | |
| **Non availability of adequate skill set and high rate of attrition** | • Absence of human management policy and strategy.<br>• Non-communication of job description/design for each employee in interview and even on appointment.<br>• Absence of policy for intra and inter rotation of staff.<br>• Restrictions on compensation packages due to Government guidelines<br>• Irrational distribution of | Low productivity.<br>Impact on competitive strength<br>Non availability of adequate skill set | 7-10<br>High | • A well-defined and documented human resource policy highlighting the recruitment system, job description, promotion criteria, employees benefits, appraisal procedure, transfer policy, welfare activities etc.<br>• Implement job design techniques which would cover job enlargement, enrichment rotation and simplification.<br>• Establish and enforce standard for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior.<br>• Job performance is periodically appraised, evaluated and reviewed with each employee. | Vice President , HR Division & HOD of all Department |

| | | | | | |
|---|---|---|---|---|---|
| | work amongst the staff and ensuring that right man is assigned the right job and contribute to organizational excellence.<br>• Absence of any time and motion studies for correlating work load with actual manpower.<br>• Identification of training needs of the employees at all levels.<br>• Engagement of contractual staff leading lack of involvement and access to the confidential data base.<br>• High rate of attrition of employees with technical qualifications.<br>• Lack of environment that rewards entrepreneurial | | | • Adopt HR tools like employee satisfaction survey, exit interviews and external benchmark study to frame and implement companywide retention policy to prevent loss of business skills and check attrition.<br>• Adopt various mechanism viz financial/non-financial rewards and recognition system including performance related incentives based on individual/ group performance which would lead to increased organizational creativity/ potential of employees, competence building aiming to have employees delight and to arrest employees attrition.<br>• Identify gaps and opportunities in human factor management (SWOT analysis) with a view to improve the process and to increase the ability of the company to compete in business market.<br>• Create second level positions in each department for continuity of work without interruption in case of non-availability of departmental | |

| | | | | | |
|---|---|---|---|---|---|
| | initiative and performance.<br>• Absence of written code of conduct and ethics with affirmations from employees to ensure compliance<br>• Absence of second line of defense for ensuring smooth and uninterrupted functioning.<br>• Absence of whistle blower policy. | | | head.<br>• Provide training to employees at regular intervals to upgrade their skills and also effectively train them in spheres other than their own specialization.<br>• Implement a written code of conduct and ethics for the employees including contractual staff and obtain affirmations from all concerned to ensure compliance.<br>• Assign responsibility and delegation of authority to deal with the companyôs goal and objectives, operating functions and regulatory requirements including information system and authorization for changes.<br>• Establish a whistle blowing and anti-fraud policy.<br>• Heads of Departments maintain contact with and consistently emphasize appropriate behavior to divisional staff.<br>• Analyse the success of the incentive programmes by qualitative and quantititative analysis and report the results of analysis to appropriate authority.<br>• Follow a policy of providing | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | equal opportunity to every employee inculcate in them a sense of belonging and commitment. A satisfie3d and committed employee will give his best and create an atmosphere that cannot be conducive to risk exposure.<br>• Employees are encouraged to make suggestions and discuss any problems with their superiors. | |
| **D. Financial Reporting Risks** | | | | | |
| **Liquidity Risk** | • Crystallization of contingent liabilities due to non-compliance with any or all the available laws, regulations, code of conduct and standards of good practices.<br>• Uncertainty in regard to interest rates at which future cash flows could be invested.<br>• Acceptance of | • Non-compliance of changing laws, regulations and standards relating to accounting and incorrect position of financial health.<br>• Liquidity crunch<br>• Under recovery of the cost resultant with loss of profit. | 7-10<br>High | • Reassess contingent liabilities and take a view to what extent these could be treated as specific liabilities<br>• Solicit expert legal opinion for cases lying in the court of law/tribunals.<br>• Proper financial planning is put in a place with detailed Annual Business Plans discussed at appropriate levels within the company.<br>• Strict compliance of the provisions of SOP. Sale of coupons to PSAs should invariable be made against realization of the amount of cheque.<br>• Based on the quantum of cheques dishonored modify SOP with the approval of appropriate authority. | Vice Presidents, Corporate Accounts, PAN Division, Southern Region Infrastructure Division and DOIT and Projects. |

| | | | | | |
|---|---|---|---|---|---|
| | cheques from PSAs (as against drafts or cash) against the provision of accepting cash or drafts.<br>• Dishonor of cheques received from PSAs.<br>• Inadequate follow up with the clients for payment of dues leading to increased provision for doubtful debts.<br>• Delay in getting refund of earnest money deposits from the clients in case of rejection of Companyôs bids.<br>• Delayed recovery of the excess amount paid to hospitals<br>Non recovery of service fee and | | | • Vigorous follow up and proactive liaising with the clients.<br>• Payment in advance of certain percentage (preferably 40-50 percent) of cost of work/project on award.<br>• Cost optimization and cost reduction initiatives.<br>• Carry out three tire reconciliation with the amount disallowed by the CGHS, recovery made from the hospitals and pending recovery.<br>• The software need to be designed to generate MIS for the amounts due from CGHS as well as hospitals.<br>• The software to have a built in provision for pending recoveries from the hospitals so that the amount could be recovered while settling the bills.<br>• Monthly bills for service fee, handling and shipping charges need to be raised by 7th of each month on the basis of settled medical claims of the hospitals.<br>• Vigorous efforts need to be put in for recovery of service fee and handling and shipping charges from CGHS | |

| | | | | | |
|---|---|---|---|---|---|
| | handling and shipping charges | | | as well as refund of earnest money from clients. | |
| **Risk of incorrect financial reporting** | • Potential human error such as carelessness, distraction, mistake of judgment, misunderstanding of instructions.<br>• Lack of accounting, internal control system and Corporate Governance.<br>• Delay in passing accounting entries.<br>• Lack of knowledge about accounting standards. | • Adverse audit opinion when financial statements are misstated.<br>• Loss of stakeholderôs confidence | 7-10 High | • All policies and procedure followed by the company should aim at protecting the assets, detection of errors and fraud, accuracy and completeness of accounting records and timely preparation of reliable financial statement.<br>• System of internal control should be reviewed to ensure that it is functioning as prescribed and is modified as is appropriate.<br>• Financial statement should be subject to quarterly audit by internal and statutory audits.<br>• Participation in trainings and seminars. | Vice President, Corporate Accounts |
| **Risk of Corporate Accounting Frauds** | • Non-compliance with rules, regulation and internal control | • Affects viability and profitability.<br>• Reputational damage and | 7-10 High | • Strong internal control by fostering control consciousness at all levels.<br>• Appropriate reporting channels. | Vice President, Corporate Accounts, PAN Division and Human Resource Department, |

| | | | | | |
|---|---|---|---|---|---|
| | system<br>• Incorrect reporting of transactions.<br>• Lack/inadequate supervision.<br>• Delayed accountal of sales of coupons to PSAs in the Tracker system.<br>• Reuse of used coupons.<br>• No updating/absence of the Delegation of Powers.<br>• Overstatement of revenue and understatement of expenditure | public embarrassment.<br>• Financial losses.<br>• Loss of key staff.<br>• Regulatory fines and penalties. | | • MIS and communication channels.<br>• Adequate protection to whistle blowers.<br>• Periodical transfers of employees/ incumbents especially where financial transactions are involved.<br>• Periodical training and information to employees on compliance issues and policies.<br>• Daily reconciliation of stock of coupons with the amount realized on sale of coupons and a certificate to this effect is recorded by the Branch in-charge.<br>• Strict compliance with the provision of SOP.<br>• Frequency of cancellation of cheques is minimum.<br>• Update/frame Delegation of powers with defined role and power at each level. | |
| **Risk of Erosion of Profit due to Government Policy** | • Withdrawal of KYC business.<br>• Fixation of rates for issue of PAN cards without correlating with the Companyôs cost<br>• Appointment of | Loss of revenue and consequent erosion of profits | 4-6<br>Medium | • Pursue with the Government for taking protective measures to mitigate the adverse effect of withdrawal of business and loss of revenue.<br>• Proactive liaising with Government Departments to maintain healthy relations | Vice Presidents PAN Division, Southern Region and Company Secretary. |

| | | | | | |
|---|---|---|---|---|---|
| | Company for clearance CGHS bills without any correlation with cost involved in processing the payment of bills. . | | | | |
| **E. Contract Management Risks** | | | | | |
| **Cost and time overruns in completion of works and its impact on competitive bidding** | • Lack/ inadequate financial scrutiny before submission of bids.<br>• Over/under estimation of time and resources.<br>• Escalation in prices of input.<br>• Commencement of work without receipt of advance payment as per the terms of contract.<br>• Delay in raising bills for work done.<br>• Non/delayed receipt of payments from the clients. | • Loss of market share and consequent loss of revenue.<br>• Impact on critical path | 7-10 High | • Ensure adequate scrutiny of the financial bid before submission of tenders to obviate the possibility of under /short recovery of cost.<br>• Develop an internal mechanism for effecting proper assessment of cost component and improve planning and execution to avoid time and cost overrun.<br>• Implement a system of regular review of cost and fix responsibility centers for cost of each project.<br>• Build Knowledge Management System which will be repository of all project related information. This system can be used to understand the reasons for cost and time overrun and estimation of new projects shall take those factors into | CTO/Vice President, DOIT/Projects and Infrastructure Division |

| | | | | | |
|---|---|---|---|---|---|
| | - Inadequate follow up of the payments from the clients.<br>- Non standardization of bidding conditions.<br>- Changes in design, material etc. based on client requirements.<br>- Delayed execution of projects by sub-contractors | | | account.<br>- Build capabilities for bidding projects by creating knowledge bank of the companyös bids as well as those put in by the competitors and identify areas where cost and time overrun can be reduced.<br>- Standardize the terms and conditions of the bidding (clients) and tender (subcontractors) documents and these are reviewed before bidding and tendering.<br>- Local constraints are factored into while preparing the cost estimates and time schedule.<br>- Proactive liaising with clients to maintain healthy relations<br>- Timely and vigorous efforts with clients for payment of the value of work done.<br>- Provide for the schedule of payments based on certification of the works in the agreements with clients.<br>- Any subsequent changes in the design after the execution of the agreement have to be billed on the basis of extra items.<br>- Provide for a penalty clause in the agreement with the sub- contractors which should be at par with that | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | indicated by the clients. | |
| | | **F. System Risks** | | | |
| **System Capability**<br>**System reliability**<br>**Data Integrity**<br>**Coordinating and interfacing** | • Inadequate investment in technological up gradation.<br>• Out sourcing the GS software maintenance, support and development services despite availability of in house adequate skill set and limited use of software.<br>• IT module does not identify CGHS claims pending at various levels and regular updating and reconciliation of the amount recouped.<br>• Non reconciliation of IT assets with the books of the Company.<br>• Intentional | Insecure IT system | 7-10<br>High | • Evaluate the technological obsolescence on continual basis and necessary investment to bring in the best prevailing technology. The companyôs policy should also include a favorable dispensation for replacement of hardware and software on a constant basis to take advantage of such technological movements<br>• Develop an IT strategy linked with long and medium term plan.<br>• Implement IT security policy to minimize disruption of IT services due malware attacks and also pilferage of information.<br>• A Disaster Recovery Site as apart of the Business Continuity Plan has been developed at an alternate site.<br>• Access to password tables is restricted to only those who really need to access the table.<br>• In a division/unit where the employee has resigned or his services have been terminated ensure that the password of such employee has been deleted and the | CTO, Vice President, DOIT/Projects |

| | | | | | | |
|---|---|---|---|---|---|---|
| | actions by former employees using knowledge gained while an employee. | | | passwords of other employees in the division/unit have been changed.<br>• Check the capability of the GS software for R&T activities of the existing mutual funds based on the guidelines issued by SEBI and AMFI.<br>• Consider the possibility of reviewing the agreement with the third party for support and development services in view of the limited use of GS for managing residual work.<br>• Evaluate the application controls with a view to ascertain the weaknesses in system software, programme and data security as such weaknesses significantly decrease the integrity of the system.<br>• Modify the system to generate MIS reports for recoupment amount pending, amount claimed, number of disallowance cases together with the reasons. This will help to closely monitor the activity relating to processing of bills under CGHS.<br>• All IT assets need to be accounted as per the | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | accounting policy and practice.<br>• Determine if the Business Continuity Plan exists and assess the degree to which it has been defined, documented, tested and maintained and communicated i regard to critical applications and processes, back up recovery and alternative operating procedures, personnel requirements, address both IT services and business operation resumption.<br>• The level of virus protection established on servers and workstations is determined and monitoring of infection is being done by IT Administration. Virus application needs to be updated on periodical basis. Laptops should be ensured to have secured internet access.<br>• Personnel should be trained to remain abreast of technological developments in their respective fields.<br>• Relying on one person to maintain networks, computer facilities and such can severely compromise the day-to-day operations if problems occur. Having the | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | necessary support structure with backup personnel is important | | |

## G. Environmental Risk

| | | | | | |
|---|---|---|---|---|---|
| Threat to property, Safety and security of people | Impact of natural calamity like floods, heavy rainfall, earthquake etc. | • Geo physical development<br>• External security threats like sabotage, terrorist attack.<br>• Inadequate/untimely information flaw from security agencies. | 1-3<br>Low | • Develop Disaster Management Plan and ensure that the Companyôs disaster plan is captured by the State Master Disaster Management Plan.<br>• Insurance against war risk, fire, flood, riots and third party losses.<br>• Improved security measures such as installation of CCTV, surveillance during day and night, effective communication channels with employees, liaison with external intelligence agencies.<br>• Insurance of property and other assets based on the value as reflected in the financial books to avoid over/under insurance.<br>• Insurance policy should cover first party losses i.e. losses which impact the insured and include asset based losses(due to natural and unnatural disaster such as fire, flood, burglary etc.) as well as financial and data losses(act infidelity by employees and computer based crimes such | Dy/Asstt. Vice President, Administration and DMC |

| | | | | | |
|---|---|---|---|---|---|
| | | | | as hacking and virus attacks)<br>• Explore the option of taking terrorism coverage policy for nullifying any loss.<br>• Regular checking of firefighting equipment and fire and bomb detection drills.<br>• Monthly safety inspection schedule and emergency evacuation plan.<br>• Security audit. | |
| ***Absence of data base of the investors.**<br>***Tax Risk** | • Payment of principal and dividend to ineligible persons<br>• Issue of duplicate certificate without proper verification of claimant.<br>• Tax Disputes<br>• Nonpayment and delayed payment of statutory dues | Noncompliance with the regulations, financial and reputation loss. | 1-3<br>Low | • Employ mechanism for multiple authorization of payment of principal and dividend to persons who have reportedly lodged claims for loss of original documents with cross checks.<br>• Adhere to internal control practices that prevent collusion and concentration of authority.<br>• Ensure strict compliance with the existing rules and regulations.<br>• Study advisories and suggestions from professional agencies, industry and regulatory bodies and where relevant. | Company Secretary. |

# CHAPTER 5

## Structure and Administration of Risk Management

## A segmented approach to risk management does not provide senior management and Board with aggregated risk management

### 5.1 Need

From an organizational standpoint, the traditional approach to managing the various risks to which the organization is exposed was to treat them separately, appointing someone to manage each risk. Executives have long tolerated this segmented approach to risk management, but they have never been really satisfied with it. From their perspective, it ignores the interdependence of many risks. It erects barriers to exploiting natural hedges among the risks and sub-optimizes the treatment of total risk.

Risk Management should not be seen as a responsibility of any particular Unit or Division rather must be seen as an enterprise wide activity. A properly designed organizational structure for managing and reporting risks is pre requisite for effective risk management process. Risk Management is a consistent and continuous process for identification and assessment of risk, deciding the control and monitoring the exposure of the risk. Risk Management is most effective when it follows a top-down approach. In this approach, the senior management is main center of power and responsibility.

"Risk intelligent management" (achieved when full advantage is taken of the potential of risk management) allows senior management and board to manage with their eyes wide open. They see around and ahead of them. They are fully aware of the potential risks, opportunities and are prepared to act decisively. Those without risk intelligence have to study the situation and hold discussions with the management team, by which time the opportunity may have passed by.

### 5.2 Structure

A proposed risk management structure is indicated below:-

(i). Board of Directors.

(ii). Risk Committee of Board

(iii). Corporate Risk Management Department (CRMD)
(iv). Risk Owners (Heads of Departments)

The defined roles and responsibilities of Board of Directors, Risk Committee of Board, Corporate Risk Management Department, Risk Owners (Heads of Departments0 and employees of UTIITSL are given in the succeeding paragraphs.

### (i) Role of the Board of Directors

The Board of Directors plays a critical role in Risk Management by establishing the right environment or tone-at-the-top. Given the Boardôs responsibilities for representing the interests of shareholders, it plays a vital role in overseeing managementôs approach to risk management.

The increase in Board risk management oversight is strengthening its ability to protect and enhance stakeholder value by way of:-

A. approval of the Risk Management, policies and procedures;
B. likelihood of such risks becoming a reality;
C. how unacceptable risks should be managed;
D. companyôs ability to minimize the probability and impact on the business;
E. costs and benefits of the risk and control activity;
F. effectiveness of the risk management process; and

### (ii). Risk Committee of Board

External drivers are encouraging Board to oversee risk management practices by assigning explicit responsibilities to Audit Committee for risk oversight to Risk Committee of Board. The Risk Committee of Board discusses policies with respect to risk assessment and risk management. While the senior management has the job of assessing and managing the Companyôs exposure to risk, the Risk Committee of Board discusses guidelines and policies (comprising of the Chairman and members of the Audit Committee) to govern the process by which this is accomplished and major financial risk exposures. Thus, the Board and Risk

Committee of Boardǿs involvement in risk management oversight is a critical component of effective governance.

Specifically, the role of Risk Committee of Board is to:

**(i).prioritize business risks** ï

a) review the risk register to understand the current risk environment for the Company, including review of emerging risks,
b) the interrelationships between risks, and in the context of Companyǿs risk appetite;
c) review and approve the proposed changes in the Risk Register.

**(ii) evaluate the effectiveness of risk mitigation activities** - review risk mitigating strategies for effectiveness and consistency with Companyǿs risk tolerance;

**(iii).ensure gaps in effectiveness are addressed for High Priority Risks** - provide direction for the allocation of resources and assignment of responsibilities for addressing business risks;

**(iii) improve Risk Management Infrastructure** - provide guidance regarding risk management infrastructure, including systems, processes, and organizational structure.

**(iv) review the process of control assessment**- results of control testing carried out by the Corporate Risk Management Department and implementation status of approved controls.

**(v) review quarterly updates-** by of way changes in key risks, related controls and action plans.

i. Risk Committee of Board will meet at such regular intervals as may be decided) for reviewing the risk and control framework implemented by the Company.

### (iii). Corporate Risk Management Department (CRMD)

#### (a). Why separate set up?

Risk management is not just about managing financial risks, such as risks relating to currency movements or changes in the price of commodities. It's not just about managing the risk of failing to comply with laws and regulations. It's not just about the risk of errors in the financial statements. It's also not just about operational and strategic risks, such as the potential failure of a sole supplier. It's about managing the potential effects of uncertainty throughout the Companyǒs business operations. In other words, it's all of the above. Whenever management and the board discuss strategies, they should be considering risk. Whenever Heads of Departments make decisions, they should be thinking about the risks and doing something about them.

Risk is not something that can be managed once each quarter or just on Fridays. Risks appear and have to be addressed all the time. They need to be integrated into routine decision-making, strategy-setting, and performance management. The Company should have a dedicated Corporate Risk Management Department which acts as the custodian of companyǒs risk architecture and its management within the prescribed policy limits.

#### (b). Composition

A separate set up known as Corporate Risk Management Department under the overall direction, control and supervision of a Vice President (preferably Company Secretary) will be set up at the corporate level which will be responsible for the day to day implementation of the risk management process. The Department will also collate updates from the Risk Owners and prepare the Management Information Reports

#### (c).Responsibility

. The main responsibilities of Corporate Risk Management Department include:

1. Implementing and maintaining appropriate risk management principles and policies, internal controls and processes designed to identify and address unacceptable risk as determined by the Risk Committee of Board.

2. Establishing an integrated risk management framework to measure and manage all aspects of risk. These risks include credit risks (such as lending and counterparty exposures); market risks (such as interest rate, foreign exchange, equity and commodity exposures);business risks (such as volatility in volumes, margins, or costs); and operational risks (ranging from day-to-day processing errors to fraud and other low probability but high severity events).
3. Ensuring that appropriate and effective risk management processes are in place within their designated area(s) and scope of responsibility.
4. Ensuring that all employees are made aware of the risks within their work environment and of their personal responsibilities.
5. Preparing specific Division policies, procedures and guidelines to ensure all necessary risk assessments are carried out within the Division in liaison with Risk Owner where necessary.
6. Implementing and monitoring any identified and appropriate risk management control measures within their designated area(s) and scope of responsibility.
7. Ensuring that all employees are given the necessary information and training to enable them to undertake effective risk management practices.
8. Reporting regularly pertinent information, including recommendations made, to the Senior Management, Board of Directors and Risk Committee of Board that support the proactive management of risk.

### (iv). Risk Owner

#### (a). Need

Policies and frameworks are fundamental tools to ready an organization for integrated risk management, but it is the people in the organization that make the practice work. Empowering employees in operational areas will help ensure success in establishing the function. These employees will assist senior management in developing work plans that reflect a corporate perspective on risk-related issues. It is also an appropriate channel for communicating implementation concepts and timing throughout the organization.

A critical aspect of successful implementation is weaving integrated risk management seamlessly into existing departmental processesð annual corporate planning, performance reporting, and training development and delivery must all be risk-attuned.

Aligning risk management vision and objectives with corporate objectives and strategic direction helps make risk management meaningful and relevant to all employees. As implementation progresses, individuals should come to understand managing risk as part of their daily work, not something superimposed on their usual activities. Acceptance of the concepts of integrated risk management will be commensurate with the extent that the organization has been successful in establishing and using common risk terminology in corporate tools and documentation.

**(b). Set up**

Risk identification is continuous process and is carried out by the employees. Heads of Departments as Risk Owners are responsible for validating the identified risks, risk assessment, risk escalating matrix, prepare and execute action plan within their own areas of responsibility. Each of the Division will nominate Nodal Officer for coordinating the risks of the respective Division. Risks identified are validated by the Risk Owners in a validation meeting with the CRMD.

**(c). Responsibility**

The main responsibilities of Risk Owners include:-

1 Timely identification and escalation of the risks in the functional domain.

2 Determine both inherent and residual risks through:

a. Determine inherent likelihood of event occurrence and severity level of the impact,
b. Engage employees in determination of the risk rating,
c. Identify the existing/required key controls for minimizing the identified risk,
d. Determine the responsibility, type, extent of control required for each identified risk,

e. Develop action plans for implementing and strengthening the related key controls.

3 Each Risk Owner should on regular basis reports on default/delay in completion of action plan, review results of compliance testing by CRMD and summery of proposed changes in the Risk Register.

# CHAPTER 6

## Risk Management Tool

### 6.1 Introduction

Most business managers have an instinctive understanding of the risks they face, and will have taken mitigating action, often without even realising it. Although this may give some practical protection against problems and disaster it can still leave a business exposed. Risk management tools allow planners to explicitly address uncertainty by identifying and generating metrics, parameterizing, prioritizing, and developing mitigations, and tracking risk. These capabilities are very difficult to track without some form of document or, with the advent of information technology, software application.

### 6.2.Management Tools

The management tool broadly comprised of:-

(A). Risk Register

(B). Management Information System

(C). Check List

#### (A). Risk Register

A **Risk Register** is a Risk Management tool commonly used in organizational risk assessments. It acts as a central repository for all risks identified by the organization and, for each risk, includes information such as risk probability, impact, counter-measures, and risk owner and so on. It can sometimes be referred to as a **Risk Log**. Risk Register formalizes the consideration of risk, and opportunities, in a way that enables wider consideration and discussion within management or at Board/Risk Committee of Board level. Although a Risk Register tends to focus on negative risks, if used sensibly it should also address the opportunities which face the business.

The purpose of a risk register is to record details of all risks that have been identified, together with their analysis and plans for how those risks are to be treated. The risk register is an important component of the overall risk management framework. It usually includes:

a) a unique identifier for each risk;

b) a description of each risk and how it will affect the project;

c) an assessment of the likelihood it will occur and the possible seriousness/impact if it does occur (low, medium, high);

d) a grading of each risk;

e) who is responsible for managing the risk;

f) an outline of proposed mitigation actions (preventative and contingency); and

g) in larger projects, costing for each mitigation strategy.

This Register should be maintained throughout the life of the organization and will change regularly as existing risks are re-graded in the light of the effectiveness of the mitigation strategy, and new risks are identified. In practice, the Risk Register is regularly reviewed and updated and may be a permanent item on the meeting agenda of the Board/ Risk Committee of Board.

Access to the risk register must be controlled to maintain its integrity and confidentiality. Some items recorded in the register may be very sensitive and thus not for wide publication. These confidential items can be 'flagged' by adding an extra field to the table record structure. The integrity of all item entries is also important, so there is a need for security policy for the register that defines who should be able to update the table and who can read it.

**(i). Need**

A *Risk Register* is developed to:

a. provide a useful tool for managing and reducing the risks identified;

b. document risk mitigation strategies being pursued in response to the identified risks and their grading in terms of likelihood and seriousness;

c. provide the Board, Risk Committee of Board, CRMD and Risk Owners with a documented framework from which risk status can be reported;

d. ensure the communication of risk management issues to key stakeholders;

e. provide a mechanism for seeking and acting on feedback to encourage the involvement of the key stakeholders; and

f. identify the mitigation actions required for implementation of the risk management plan.

### (ii). Risk Register Template

A sample risk register, in the form of a table, is shown below. This table could be maintained as a simple document in either a word-processing format or a spreadsheet format, but it is more likely to be stored in a database. Each risk entry in the table has a unique identifier to avoid any confusion in cross-referencing risks to other documents.

| Sr. No. | Nature of entry | Explanation |
|---|---|---|
| 1. | Content | Description |
| 2. | Risk name | Name of the risk |
| 3 | Scope of the risk | Description of risk with details |
| 4 | Nature of risk | What sector of risk fits according to business definition(e.g. Operational, Strategic, Finance, IT, Compliance) |
| 5 | Stakeholders | Who are the stakeholders affected and what degree. |
| 6. | Owner | Who owns the risk. |
| 7. | Risk impact | What is the impact of risk. |
| 8. | Probability of occurrence | What is the probability of the event occurring. |
| 9. | Risk level | What is the risk level(a function of impact and probability) |
| 10. | Risk treatment | What measures are in place to address the risk |
| 11. | Action to be taken | Any action to be taken. |
| 12. | Date identified | Date on which identified. |
| 13. | Date of entry in the register | Date on which added to the register |
| 14. | Due by | By what date |
| 15. | Review date | Date of review of the risk |
| 16. | Date closed | Date on which risk entry closed. |
| 17. | Closed by | Who authorised the closing of the risk |

### (iii). Compiling a Risk Register

The process of compiling the register will probably start off by identifying a wide variety of risks, but these should then be filtered to allow the company to concentrate on those with the greatest potential impact, so that what is presented to the Board/ Risk Committee of Board will be refined to perhaps important key risks/opportunities.

How a Risk Register is compiled will depend on the complexity of the business, but it is usually sensible to start from the ground up, either with departments, sites or business entities within the organization. This information will be based on what is important to each one, but the documents are consolidated as they move up through the organization and filters are applied, so that what is presented to the Board/ Risk Committee of Board will cover only those risks/opportunities which will have the filtered impact on the company as a whole. If the exercise is carried out appropriately it will, however, give management throughout the organization the opportunity to take a formal look at the specific risks they face and how they deal with them. It is also important to emphasize that this is not a scientific exercise, and that although one attempts to quantify risks, to a great extent this is done on a subjective basis.

Even more important than putting the register together ï which must, however, be done diligently ï is the use to which it is put. It should not be viewed simply as another box ticked, but as something that will help management and the Board/ Risk Committee of Board to ensure that their risk policies are appropriate. It will rarely identify every risk that a business faces.

### (B) .Risk Management Information System (MIS)

An enterprise-wide integrated Risk Management Information System (MIS) needs to be implemented by the company. The report captures the various delays and the key reasons for the same. However, such information is needed at all levels of the organization to identify, assess and respond to future occurrences of risk events. Pertinent information from both internal and external sources must be captured and shared in a form and timeframe that equips personnel to react quickly and efficiently. Effective communication would also involve the exchange of relevant data with external parties, such as customers, vendors, regulators and shareholders. Further, both historical and current data needs to be collected. Historical data tracks actual performance against target, identifies trends, correlate results and forecasts performance. Historical data also provides early warning signals concerning potential risk-related events.

Current data gives management a real time view of risks inherent in a process, function or unit. This will enable the company to alter its activities as needed in keeping with its risk appetite..

The reporting structure of the MIS will be as follows:

| **Authority** | **Function level** | **Reporting to** | **Risk Escalation** |
|---|---|---|---|
| Board | | | Risk Committee of Board submits report to Board |
| ⇧ | | | |
| Risk Committee of Board | Corporate | Board | To be escalated on the basis of need, impact level and exigency of situation.<br>Regular review and monitoring of the key risk and the Risk Management System |
| ⇧ | | | |
| Corporate Risk Management Department | Corporate | Risk Evaluation Committee | To be escalated on the basis of need, impact level and exigency of situation |
| ⇧ | | | |
| Risk Owners | All Heads of Departments and Regional Managers | Corporate Risk Management Department | All risks are to be reported as per Risk Register |

Each Risk Owner will submit the report to Corporate Risk Management Department in the pro forma indicated below on quarterly basis (preferably by 7th of each quarter). The Corporate Risk Management Department on receipt of the report from the Risk Owners will put up these reports to the Risk Committee of Board in its quarterly meeting. A format of Management Information Report for submission to CRMD by the Risk Owner and Audit to Risk Committee of Board by the CRMD are given below:-

## Management Information Report for submission

### Part A

### Report of the Corporate Risk Management Department to Risk Committee of Board

| Name of Department | Name and brief details of Risk | Rated As | Risk Owner |
|---|---|---|---|

### Part B

### Risk being followed up by the Corporate Risk Management Department for information of Risk Committee of Board

| Name Of Department | Nature of Risk | Risk Rating/Grade | Risk Mitigation Action | Periodicity of Risk | Risk Owner |
|---|---|---|---|---|---|

### Part C

### Risk being followed up by the Risk Owner for information of Corporate Risk Management Department

| Name Of Department | Nature of Risk | Risk Rating/Grade | Risk Mitigation Action | Periodicity of Risk | Risk Owner |
|---|---|---|---|---|---|

### C. Check list

The Checklist has been developed to assist Heads of Departments begin implementing Risk management into their groups. Every group has differing risks and needs to ensure that these are identified and managed. The purpose of the document is to provide a quick reference check list/agenda for use by the Heads of Departments to ensure that appropriate activities related to risk management have been addressed.

The format of the check list has been designed to guide the Risk Management process. The check list has been divided in three groups and each group has certain set of questions which have been classified as óEssentialô and óAdvanceô. The questions marked as óEssentialô are important from the point of view of the Risk Management framework while questions categorized as óAdvanceô talk about the management preparedness for development, implementation and monitoring the risk management.

The check list is not a substitute for understanding of risk management process nor reduces the responsibility of the Risk Owners for thoroughness. It serves only as a guide intended to help organize the risk management process. The check list is not exhaustive and should be reviewed updated regularly based on the lessons learnt.

| **Sr. No.** | **Section** | **Requirement** | **Essential(E)/Advance(A)** | **In place (yes/No)** |
|---|---|---|---|---|
| **1. DEVELOPING A RISK MANAGEMENT FRAMEWORK** | | | | |
| **1** | Communicate and Consult | Has the board and executive expressed their support for a risk management programme? | E | |
| **2** | Establish the Context | Have you identified a person(s) who will be responsible for implementing risk management? | E | |
| **3** | Establish the Context | Does the risk owner, or equivalent, have reasonable access to staff and management across the organization? | E | |
| **4** | Establish the Context | Have you defined categories of risk relevant to your Division/unit | E | |
| **5** | Establish the context | Do your risk categories reflect all operational risk areas of the business as well as more strategic risk categories? | E | |
| **6** | Establish the Context | Is there a clear organizational strategy (or objectives) articulated for the organization? | A | |
| **7** | Establish the Context | Have you defined and agreed a likelihood scale to assess the potential for the risk to occur throughout the organization? | E | |
| **8** | Establish the Context | Have you defined and agreed a consequence scale to help assess risk impacts across the organization? | E | |
| **9** | Establish the Context | Does the organizationôs consequence scale describe both financial and non-financial impacts? | E | |
| **10** | Establish the | Does the risk Management | E | |

| | | | | |
|---|---|---|---|---|
| | Context | framework consider the effectiveness of controls or risk treatments? | | |
| **11** | Establish the Context | Is there an agreed template or format for recording risks and risk treatment information (a risk register)? | E | |
| **12** | Establish the Context | Has a risk policy been defined? | E | |
| **13** | Establish the Context | Does the organization have a documented risk management strategy? | A | |
| **14** | Communicate and Consult | Have the Corporate Risk Management Department and the board/Risk Committee of Board reviewed and approved the risk policy/ strategy? | E | |
| **15** | Establish the Context | Do job descriptions of key stakeholders include responsibilities for risk management? | E | |
| **16** | Establish the Context | Is a formal project management methodology used to manage projects? | A | |
| **17** | Establish the Context | Is a mechanism in place to identify, assess, record and monitor risks? | A | |
| **18** | Establish the Context | Has the organization agreed what types and levels of risk are unacceptable? | E | |
| **19** | Establish the Context | Are there an agreed format/ template for reporting on risk? | E | |
| **20** | Establish the Context | Is there a process and/or template where new risks can be recorded by the management? | E | |
| **2. IMPLEMENTING A RISK MANAGEMENT FRAMEWORK** | | | | |
| **21** | Communicate and Consult | Is risk management or awareness training provided to all staff? | E | |
| **22** | Communicate and Consult | Does the risk owner (or equivalent) have access to the CEO, board and Risk Committee of Board when required? | E | |
| **23** | Communicate and Consult | Does staff know that they have a right and responsibility to assist in risk identification and escalation? | E | |
| **24** | Communicate | Does staff know who to report/ | E | |

| | | | | |
|---|---|---|---|---|
| | and Consult | escalate risks? | | |
| **25** | Communicate and Consult | Do managers or supervisors know that they are responsible for managing risk in their area/s of responsibility? | E | |
| **26** | Communicate and Consult | Have the executive and the board provided guidance on what information they would like to see in risk reports? | E | |
| **27** | Communicate and Consult | Is there agreement on when and how often risk reports will be produced? | E | |
| **28** | Communicate and Consult | Have the recipients of risk reports been identified and agreed? | E | |
| **29** | Communicate and Consult | Can different risk reports be produced to meet different needs of stakeholder groups? | A | |
| **30** | Communicate and consult | Has responsibility for managing/ treating specific risks been assigned and communicated to those responsible? | E | |
| **31** | Communicate and Consult | Are staff encouraged or incentivized to report risk or suggest risk reduction strategies? | A | |
| **32** | Risk Assessment | Has a risk brainstorming workshop (or workshops) been conducted? | E | |
| **33** | Risk Assessment | Have you considered the history of events and incidents in the organization during the risk assessment process? | A | |
| **34** | Risk Assessment | Has research been performed to understand common risks in the industry? | A | |
| **35** | Risk Assessment | Has the executive and board considered risks relating to the achievement of key organizational goals and objectives? | A | |
| **36** | Risk Assessment | Are risks identified during compliance reviews/ audits always added to the risk register? | E | |
| **37** | Risk Assessment | Have existing controls been identified for risks during the risk assessment process? | E | |
| **38** | Risk Assessment | Has the perceived effectiveness of controls been assessed by a person who understands the risk and the | E | |

| | | | | |
|---|---|---|---|---|
| | | controls in place? | | |
| **39** | Treat Risks | Does the risk register record the job title of the person responsible for overseeing the risk treatment and monitoring process (the 'risk owner')? | E | |
| **40** | Treat Risks | Have you identified possible actions/ treatment plans that could help to reduce the risk level? | E | |
| **41** | Treat Risks | Have the benefits of a treatment approach been compared to the potential cost of the risk to determine the appropriateness of the treatment strategy? | A | |
| **42** | Treat Risks | Have risk treatment or action plans been documented and approved for important risks? | E | |
| **43** | Treat Risks | Have due dates/ completion dates been agreed for risk treatment actions and plans? | E | |
| **44** | Treat Risks | Is there a clear understanding of who will oversee the risk treatment selection and execution process? | E | |
| **45** | Treat Risks | Have key risk indicators (KRIs) been defined and agreed for key risks/ risk areas? | A | |
| **46** | Treat Risks | Are the organizationôs physical assets appropriately insured? | E | |
| **47** | Treat Risks | Is a business continuity plan (BCP) in place for critical organizational functions/ processes? | A | |
| **48** | Risk Assessment | Has the risk register been updated in the last year? | E | |
| **49** | Risk Assessment | Is the risk register updated throughout the year to reflect changes in risk and emerging risks? | A | |
| **3. MONITORING AND REVIEW/ ENHANCEMENT OF A RISK MANAGEMENT FRAMEWORK** | | | | |
| **50** | Monitor and Review | Does the Internal Audit function or equivalent review risk management processes? | A | |
| **51** | Monitor and Review | Are an Internal Audit function/ process in place? | E | |

| | | | | |
|---|---|---|---|---|
| **52** | Monitor and Review | Does your internal audit focus its time and effort on the most critical risks recorded in the risk register? | A | |
| **53** | Monitor and Review | Does the organization track changes in risk levels over time in order to understand trends/ changes in risk levels? | A | |
| **54** | Monitor and Review | Has the risk policy been reviewed and approved in the last year? | E | |
| **55** | Monitor and Review | Has the board/audit committee and/or risk evaluation committee (or equivalent) made an attestation in the annual report on Risk Management Framework | E | |
| **56** | Monitor and Review | Is the risk process integrated with other organizational planning processes - for example is risk considered during the strategic planning, budgeting and audit planning processes? | A | |

# CHAPTER 7

## INTERNAL AUDIT IN RELATION TO RISK MANAGEMENT

### 7.1. Introduction

The importance to strong corporate governance of managing risk has been increasingly acknowledged. Organizations are under pressure to identify all the business risks they face; social, ethical and environmental as well as financial and operational, and to explain how they manage them to an acceptable level. Meanwhile, the use of enterprise-wide risk management frameworks has expanded, as organizations recognize their advantages over less coordinated approaches to risk management.

Internal audit is a valuable resource to the management, Board of Directors and Audit Committee in accomplishing overall organizational goals and objectives and simultaneously strengthening internal control and overall governance. In the current global scenario internal audit reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and effective use of resources and established operational goals and objectives.

### 7.2. Role in Risk Management

Internal audit role in risk management is achieved through:-

(a). Providing Assurance.

(b). Consulting Role.

The key factors to take into account when determining internal audit role are whether the activity raises any threats to the internal audit independence and objectivity and whether it is likely to improve the companyҫs risk management, control and governance processes. Internal audit expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that the internal audit is well qualified to act as champion and even project manager for risk management, especially in the early stages of its introduction. As the organizationҫs risk maturity increases and risk management becomes more embedded in the operations of the business, internal audit role in championing risk management may reduce.

### (a). Providing Assurance

One of the key requirements of the Board of Directors and the Audit Committee is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level. It is likely that assurance will come from different sources. Of these, assurance from management is fundamental. This should be complemented by the provision of objective assurance, for which the internal audit is a key source. Internal audit will normally provide assurances on three areas:

a. Risk management processes, both its design and how well it is working;
b. Management of those risks classified as ˆkeyˆ, including the effectiveness of the controls and other responses to them; and
c. Reliable and appropriate assessment of risks and reporting of risk and control status.

Internal audit is an independent, objective assurance and consulting activity. Its core role with regard to risk management is to provide objective assurance to the Board of Directors and the Audit Committee on the effectiveness of risk management. Indeed, the two most important ways that internal audit provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively.

By providing assurance on the risk management, control, and governance processes within an organization, internal audit is one of the key cornerstones of effective governance.

### (b). Consulting Role

Internal audit provide consulting services that improve companyˆs governance, risk management, and control processes. The extent of internal audit consulting role in risk management depend on the other resources, internal and external, available to the Board/Audit Committee and on the risk maturity of the organization and it is likely to vary over time.. Some of the consulting roles that the internal audit may undertake are:-:

I. making available to management tools and techniques used by internal audit to analyze risks and controls;

II. being a champion for introducing risk management into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization;

III. providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding;

IV. acting as the central point for coordinating, monitoring and reporting on risks; and

V. supporting Departmental Heads as they work to identify the best way to mitigate a risk.

The key factor in deciding whether consulting services are compatible with the assurance role is to determine whether the internal audit is assuming any management responsibility. In the case of risk management, internal audit can provide consulting services so long as it has no role in actually managing risks ï that is managementôs responsibility ï and so long as senior management actively endorses and supports risk management. Whenever the internal audit acts to help the management to set up or to improve risk management processes, its plan of work should include a clear strategy and timeline for migrating the responsibility for these services to management.

### **7.3**. **Safeguards**

Internal audit may extend its involvement in risk management subject to following conditions:-:

(i) It should be clear that management remains responsible for risk management.

(ii) The nature of internal audit responsibilities should be documented in the internal audit charter and approved by the audit committee.

(iii) Internal audit should not manage any of the risks on behalf of management.

(iv) Internal audit should provide advice, challenge and support to managementôs decision making, as opposed to taking risk management decisions themselves.

(v) Internal audit cannot also give objective assurance on any part of the risk management framework for which it is responsible.

(vi) Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

## 7.4 Audit Guidelines

Internal Audit guidelines are given below:-

### (A). In relation to Internal Control

While the management is responsible for establishment and maintenance of appropriate internal control and risk management system, the role of internal auditor is to suggest improvements to those systems. For this purpose the internal auditor should:-

(i) Obtain an understanding of the risk management and internal control framework established and implemented by the management,

(ii) Perform steps for assessing the adequacy of the framework in relation to organizational set up and structure,

(iii)Review the adequacy of the framework.

### (B).In relation to Risk Management System

i. Obtain document containing the risk management framework and accordingly ascertain that the process is both comprehensive and suitable for the Company.

ii. Review background information on risk management methodology and other material used as a base with a view to assess whether the process adopted by the management is appropriate and represent the best practice of the industry.

iii. Ascertain that the risk management procedures are clearly understood by all key levels involved in risk management process.

iv. Review Companyös policies, Board of Directors and Audit Committee minutes to determine the Companyös business strategies, risk management philosophy and methodology, appetite and acceptance for risk.

v. Assist in planning the procedures in risk management framework based on his specialized knowledge of the Company.

vi. Examine, evaluate, report and recommend improvements on the adequacy and effectiveness of managementôs risk processes.

vii. Assess whether the risk management framework has to be updated and whether any improvement in the risk management process is needed.

viii. Assess how well the risks identified by the management have been managed and prioritized in order of their significance.

ix. Ascertain whether even events with relatively low possibility of occurrence has been identified and considered if the impact of achieving an important objective is great.

x. Ensure that the system of risk treatment has been designed to bring anticipated risk likelihood and impact within the tolerance limit.

xi. Participate in the monitoring and reporting activities in the risk management process.

xii. Provide training to the Risk Owners, staff of Corporate Risk Management Department and members of the Risk Evaluation Committee.

xiii. Check that the risk management process is both timely and effective.

xiv. Ensure that the significant deficiencies noticed in risk management process are clearly brought out in the internal audit report.

xv. Examine the business continuity plan and ensure that comprehensive disaster plan exists.

.

**(C). In relation to Risk Owners (Heads of Departments)**

i. Check the efficacy and implementation status of each identified risk, as reported, on periodical basis, by the Risk Owners to the Corporate Risk Management Department.

ii. Obtain and verify the reasons for delay or default in furnishing the implementation status to Corporate Risk Management Department.

iii. Obtain and verify information received from various Risk Owners with regard to difficulties in implementation of mitigation factors/action plan.

iv. Check/test the criteria approved by Corporate Risk Management Department for assessing the implementation of the risk minimizing procedure.

v. Check, verify and report on the adequacy and accuracy of the risk control records (Risk Register) maintained by the Risk Owners.

vi. Check the efficacy of changes made in the risk profile, risk appetite and risk management process due to change in business, operating and regulatory environments.

**(D). In relation to Corporate Risk Management Department**.

i. Check and ensure that the Action Taken Notes received from the Risk Owners are properly consolidated along with the reasons for delays and defaults for submission to Risk Evaluation Committee.

ii. Check that the changes in the risks, related controls and action plan based on the quarterly reports from the Risk Owners are escalated to the Risk Evaluation Committee.

iii. Check the Corporate Risk Management Department has updated the Risk Register in terms of the approvals of the Risk Evaluation Committee and Audit Committee.

iv. Check that the periodical reports are submitted to the Board of Directors based on the recommendations of the Audit Committee. Also check that the decision of the Board/Audit Committee is being duly implemented.

### 7.5 Internal Audit Reporting

The primary object of the internal audit report is to effectively communicate the results of audit. Reporting aims are:-

1. to be within a risk assessment framework to enable comparison of reports.
2. to be supported by the audit approach.
3. to provide clear conclusions and approach.
4. to clearly express priority and significance of recommendations made.

The internal audit report should be as broadly divided into different sections and each section should cover as under:-

| | |
|---|---|
| **Section : A-1-General** | Overview of the Report |
| **Section : A-2-General** | Issues to be brought to the specific notice of senior management/MD&CEO /Audit Committee |
| **Section : B- General** | Name of the Risk Owner, number of risks identified, its management and prioritized in order of significance, number of risks actually audited and date of audit |
| **Section: C- Audit Observations** | Significant deficiencies noticed in risk management, delays or defaults in furnishing the implementation status to CRMD, adequacy and accuracy of the risk control records (Risk Register), consolidation of Action Taken Notes received from the Risk Owners along with the reasons for delays and defaults in submission to REC, implementation status of the decisions/recommendations of the Board/Audit Committee. risk management training and involvement of employees at working level |
| **Section. D-General** | Recommend improvements on the adequacy and effectiveness of managementôs risk processes. |
| **Section. E-1-Audit Procedure** | Tools and techniques used by internal audit to analyze risks and controls; |
| **Section. E-2-Follow up of outstanding audit findings** | Management action in implementing and reporting outcomes to agreed actions remedying the audit finding as per the action plan and the time table agreed with internal audit |

## 7.6. Good practice checklist for assessing Risk Management

This good practice checklist has been designed as a guide for internal audit.

The checklist is designed to promote good practice in risk management, and could be of value in the following ways:

- help UTIITSL improve and embed their own risk management arrangements
- help internal auditors in their own reviews of risk management

- maximize  the benefits they achieve from risk management, for example by producing better, more credible information
- help senior management, Audit Committees and Board of Directors assess the effectiveness of the internal control system

The attached checklist contains various questions on the adequacy of the risk management process in UTIITSL. Most invite a Yes/No answer, with space provided to explain how that conclusion has been reached. This space may also be used to identify how the risk management arrangements might be developed or improved

**UTI Infrastructure Technology And Services Ltd.**
**(Internal Audit Department)**

I. Name of the Department;
II. Name of the Risk Owner
III. No of risk identified
IV. No of risk as per Risk register
V. No risk audited with brief details
VI. Brief details of risks considered by REC/Audit Committee

## Risk Management Review

| Elements of risk management | Is this element clearly in place | | Evidence / Knowledge / Comments / Assessment / Ideas for improvement of current process |
|---|---|---|---|
| | YES | NO | |
| Overall, has the management identified and prioritized its risks to a sufficient standard, bearing in mind how far its risk management processes have come? | | | |
| Has the management identified and prioritized its high level key risks? | | | |
| Are the managementôs key risks linked to its strategic objectives | | | |
| 4 Did the key risk identification process include adequate participation from:<br>a. Board of Directors/Audit Committee<br>b Senior management team<br>c. Other senior managers<br>d. Other staff as appropriate | | | |
| Has responsibility for the oversight of individual key risks been assigned to appropriate managers?<br>(Note that, ideally, responsibility for an objective should determine who has oversight responsibility for the associated risks. Where a risk cuts across several objectives, the responsibility should be assigned to the most appropriate person.) | | | |
| Does awareness of, and responsibility for, the companyôs key risks follow the companyôs objectives in a hierarchical way, e g the objectives are cascaded down to divisions, regions, employees, projects etc | | | |

| | | | |
|---|---|---|---|
| Are risks prioritized?<br>If so, is account taken of:<br>• The likelihood of occurrence?<br>• The impact if it does occur?<br>• The timing of any impact (immediate or medium/long term)?<br>• The potential value (financial or nonfinancial) of any impact?<br>All of the above are best considered before assessing how the risk is mitigated. | | | |
| • The likelihood of occurrence?<br>• The impact if it does occur?<br>• The timing of any impact (immediate or medium/long term)?<br>• The potential value (financial or nonfinancial) of any impact?<br>All of the above are best considered before assessing how the risk is mitigated. | | | |
| Overall, has the management considered the adequacy with which it mitigates its key risks, through control mechanisms?<br>For the key risks, have all the residual risks been formally considered for compatibility with the companyøs stated risk appetite? And has the institution considered how residual risks should be mitigated?, e.g. should they be:<br>Tolerated/fully accepted without monitoring.<br>Tolerated/fully accepted with monitoring.<br>Subject to further consideration or kept under periodic review.<br>Transferred, e.g. by insurance or to a third party.<br>Subject to further action to contain the risk to an acceptable level.<br>Subject to the establishment of an early warning indicator (key risk indicator).<br>Terminated, i.e. the activity remains too risky to carry on. | | | |
| Overall, does the risk management reporting process give the senior management, Audit Committee and the Board sufficient information on risk and control to be able to make the required | | | |

| | | | |
|---|---|---|---|
| statement in the annual accounts? | | | |
| Have formal risk management monitoring and reporting arrangements been put in place.<br>For the Board/Audit Committee?<br>For the senior management team?<br>Are these adequate? | | | |
| Are risk and risk management adequately addressed in:<br>Board/Audit Committee papers?<br>Senior management team agenda papers | | | |
| Has the Company embedded risk management into its planning and operational processes to a sufficient extent**?** | | | |
| Do the following documents adequately deal with risk management:<br>Scheme of delegation.<br>Financial Regulations.<br>Budget holder guidance.<br>Project management guidance? | | | |
| Has internal audit changed its audit approach as a result of emphasis on risk management to reflect the latest good practice guidance and standards | | | |
| Has internal audit conducted any audits on the key risks as part of its audit strategy? Have the issues arising from these audits been brought to the attention of the Board, Audit Committee or senior management as appropriate | | | |
| Do external auditors have involvement in the risk management process?<br>Do they contribute to the feedback mechanisms? | | | |
| Do internal audit reports specifically report on controls versus risks? | | | |
| Is the companyôs overall approach to risk management, as assessed for the whole year and at the year-end, adequate for the business and its specific obligations? | | | |
| Has the company applied sufficient resources to risk management and its development | | | |
| Is the Audit Committee satisfied with the overall approach to risk management? | | | |

| | | | |
|---|---|---|---|
| Is there an individual in the institution with an overview responsibility for risk management | | | |
| Has the company clearly established what its high-level risk appetite is?<br>Is this reflected in its high-level risk portfolio?<br>Is the risk portfolio appropriately balanced? | | | |
| Does the management understand what its risk exposure is (it is usually at least the sum total of the residual risks identified? | | | |
| Has the management used risk management to identify opportunities for risk-taking? | | | |
| Does the company has a formal risk register?<br>Is there an adequate process for reviewing the risk register and its contents? | | | |
| Where appropriate, has the company identified relevant early warning indicators for its key risks?<br>Do these get reviewed at management level? | | | |
| Has the management adequately considered both financial and non-financial risks, e.g., reputation, fraud, health and safety, business continuity? | | | |

# CHAPTER 8

## Periodicity of Review of Risk

### 8.1. Introduction

A risk review involves re-examination of all risks to ensure that the current assessment remain valid and reviews the progress of risk reduction actions. This is because the costs and impacts of some risks may change, other risks may become obsolete, and new risks may appear. These reviews will involve re-doing Risk Analysis, as well as testing systems and plans appropriately.

### 8.2. Periodicity

The following table indicates the risk category, risk and the periodicity of reporting of risk:-

| Category of Risk | Risk | Periodicity of reporting |
|---|---|---|
| Business Environment and Industry Risks | Threat to market share | Quarterly |
| | Dependence on single client | |
| | Reputation Risk (Poor brand perception). | |
| Strategic Business Risks | Operational Risk | Quarterly |
| .Human Resource Risks | Non availability of adequate skill set and high rate of attrition | Half yearly |
| Financial Reporting Risks | Liquidity Risk | Monthly |
| | Risk of incorrect financial reporting | Quarterly |
| | Risk of Corporate Accounting Frauds | Monthly |
| | Risk of Erosion of Profit due to Government Policy | Quarterly |
| Contract Management Risks | Cost and time overruns in completion of works and its impact on competitive bidding | Monthly |
| System Risks | System Capability<br>System reliability<br>Data Integrity<br>Coordinating and interfacing | Quarterly |
| Environmental Risk | Threat to property, Safety and security of people | Half yearly |
| Legal Risk | Absence of data base of the investors.<br>Tax Risk | Half yearly |

These are broad parameter for review of risks at different stages which need to be reviewed and modified to the extent necessary.