RISK MANAGEMENT POLICY

Revision 0	**25 June 2014**
Revision	**Date**

Contents

1. OBJECTIVE

The objective of the Risk Management Policy is to lay down procedures and guidelines to assess risk and have mitigation plans in place. It should also provide the Role Mapping for the authorities responsible. The Policy basically sets out the company's approach to risk and should detail the Risk Management process to the staff and concerned representatives.

The policy should ensure sustainable business growth as it gives the mechanism for dealing with the different types of risks that the business could encounter going forward. It gives a structured approach, following which would minimize the impact of the risks. The policy identifies the various risks that could impact the business and its operations and gives a strategy to avoid, reduce, transfer or accept the respective risk.

2. DEFINITIONS

Risk

Risk is defined as the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected.

Risk Management

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

Risk Management Policy

A policy statement defines a general commitment, direction, or intention. A risk management policy statement expresses an organization's commitment to risk management and clarifies its general direction or intention.

Risk Owner

A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

Risk Assessment

Risk assessment is a process that is, in turn, made up of three processes: risk identification, risk analysis, and risk evaluation.

Risk identification is a process that is used to find, recognize, and describe the risks that could affect the achievement of objectives.

Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist.

Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.

Risk Register

Risk Register is defined as an archive that captures all the identified risks, evaluation of the risk before mitigation measures, and evaluation of the risk after mitigation measures.

3. RISK MANAGEMENT FRAMEWORK

3.1 Risk Classification & Categories

The first step in the Framework would be to Identify and Classify Risks. Risks are broadly classified into the following buckets:

3.1.1 Business Risk

The Business Risks includes the risks specific to the industry (industry, market, technology advancements, etc), counterparty risks (risks to supplier, client, and other JV partners, their suppliers, clients and business), and risks from resources (sourcing decisions, capital expenditure utilization, etc).

3.1.2 Strategic Risk

The Strategic Risks include risks from competing firms, social trends, capital availability (making the right corporate finance decisions), and business mix (selecting products with high growth expectations).

3.1.3 Operations Risk

The Operations Risks include customer related risks such as Customer Satisfaction, product failure, integrity, and reputational risk. It also includes finance related risks such as pricing risk, asset risk, currency risk, and liquidity risk

3.1.4 Risk from Regulatory Environment

The risks from Regulatory Environment include all the risks that arise from adverse developments in the regulatory scenario, and the political environment in all the countries involved in the functioning of the business.

3.1.5 Societal Risk

The Societal Risks include the risks from environmental interactions of the Business (carbon emissions, water and energy depletion, hazardous waste disposal, etc), society (impact of projects on communities), and natural disasters.

After identifying the risk, the next step would be to categorize the risks using a traffic light mechanism as shown below and follow the risk management process.

Traffic Light	Risk Type	Risk Effect
	High	70% to 100%
	Medium	30% to 70%
	Low	0% to 30%

Thorough analyses and classification of the different risks that our firm faces are given in **Annex-1**.

3.2 Risk Management Process

The Risk Management Process provides a framework for more efficient use of capital and resources, improving decision making and planning, reducing volatility, improving operational efficiency, and developing human capital. The process includes steps to identify the risks, assess the risks, evaluate the risks, report it, formulate a decision, mitigate the risk, and frequently monitor the entire system.

Risk Identification

Risk identification can be defined as the process that identifies an organization's exposure to uncertainty. This requires an in-depth knowledge of the market, industry, products and processes, legal, social, political, and cultural environments in which the business is operated in.

The risks need to be comprehensively identified to cover all the areas where risks can be expected to arise from. It should be approached in a methodical manner in order to ensure that all significant activities and risks related to them are covered in this process. This can be done by a detailed discussion with Risk Owners and the internal Risk Management Committee, and risk analysis in the specific industry. Also, compliance with Government Policies, Laws & Regulations, such as the Safety Regulations in the Factories Act, needs to be ensured.

The above sub-topic on "Risk Classification & Categories" also elaborates on Risk Identification.

The process is followed as per section 4. Roles & Responsibilities

Risk Assessment & Evaluation

The Risk Assessment and Evaluation process can be considered to be qualitative or quantitative in nature. It should take into account two contributing factors – the probability of occurrence of the event and the impact of such an occurrence.

The risks can be analyzed by using many different techniques: R&D, Business Impact Analysis, SWOT Analysis, Fishbone and FMEA.

Risk assessment and evaluation also includes the categorization of each type of risk into the 3 buckets (Traffic Light) of high risk, medium risk, and low risk based on the analysis done on these risks.

The process is followed as per section 4. Roles & Responsibilities

Risk Reporting

Once all the risks are identified and evaluated, they need to be recorded. This process of recording all the risks that can be perceived to impact the business in a Risk Register is called Risk Reporting. The Risk Register has to be populated by the Risk Owners and this Risk Register should be presented to the Internal Management Committee, Risk Management Committee, Audit Committee and the Board Members whenever the register is updated

A sample from the Risk Register is illustrated in **Annex 2**.

It should also be decided in this step, what is the best way of dealing with the risk. The different ways to handle or treat risks are:

1. Avoidance
2. Reduction
3. Alternate Actions
4. Share or insure
5. Accept

The process is followed as per section 4. Roles & Responsibilities

Risk Mitigation and Monitoring

Risk Mitigation and Monitoring is the process of selecting and implementing measures to modify/ reduce the risk and putting in place internal controls to monitor the risk regularly. The effectiveness of the internal control gives the degree to which the risk will be eliminated or reduced by the specific control measure. The mitigation plan should be cost effective in the sense that the cost of implementing the measure should be lower than the expected risk reduction benefits.

The cost of implementing and monitoring a specific measure can be accurately measured and this will act as a benchmark for the cost effectiveness. The expected loss from the risk without any control measure should also be arrived at. Based on these two values the management can decide on whether or not to implement the specific mitigation measure.

An effective Risk Management process requires a good reporting and review mechanism. The risks are identified, assessed and evaluated, reported, and a risk mitigation plan implemented. Regular audits of policies and the systems in place are

required to ensure compliance with the mitigation plan and the risk management policy. The business operates in a dynamic environment and this means that there must be change management process in place to check and implement changes to policies and processes as there are changes in the environment.

The process is followed as per section 4. Roles & Responsibilities

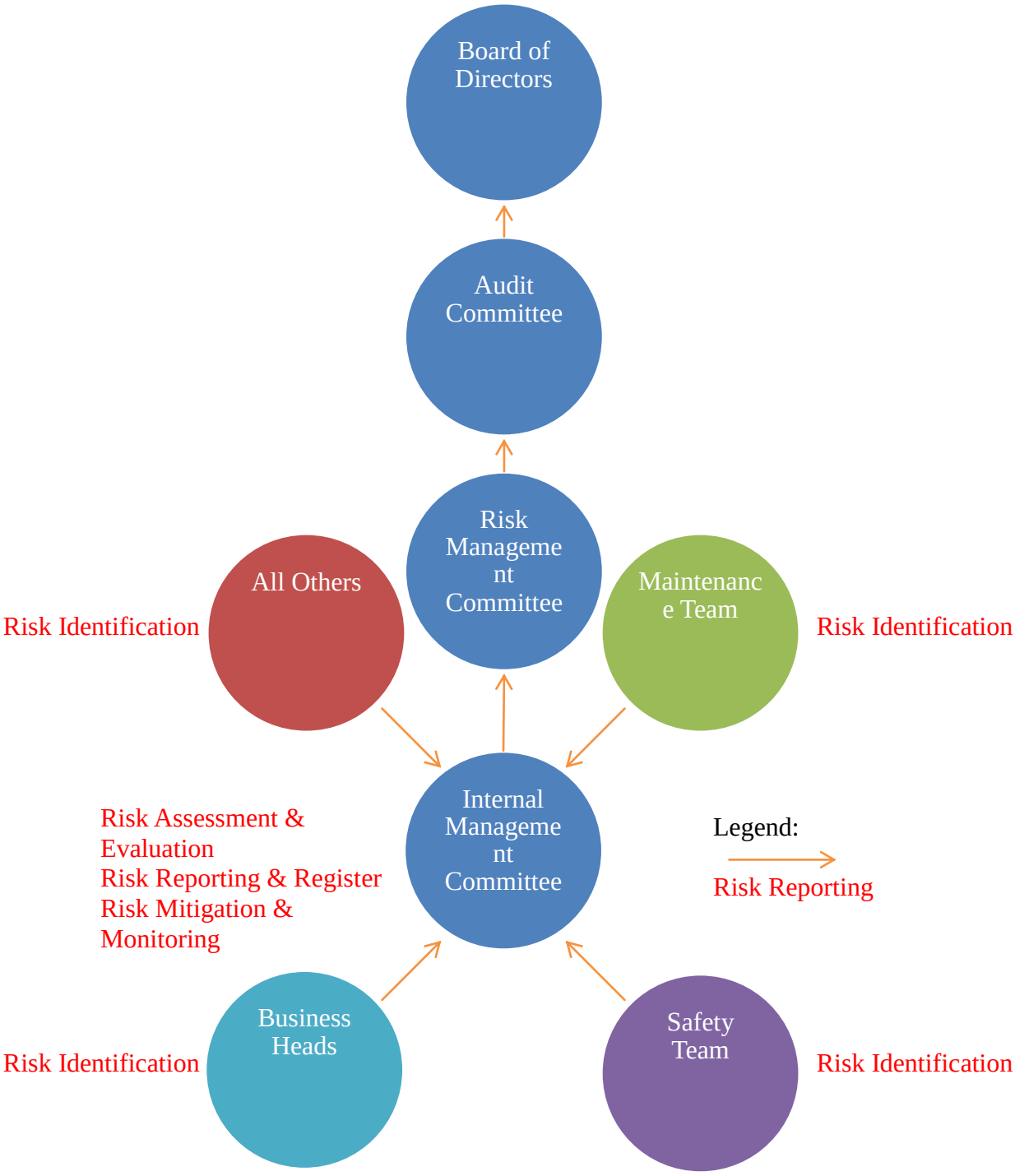
3.3 Legal

Compliance to Laws and Regulations is not an option. The laws and regulations have to be properly comprehended and systems of controls have to be implemented to achieve compliance.

3.4 Fraud

Fraud Risk Management is crucial to fraud control, guiding the development of an effective fraud control plan and associated strategies and activities to minimize the opportunities for fraud to occur. It provides a framework to identify, analyze, evaluate, and handle fraud risks. For more details, refer “IMIL_RM_Fraud.doc”.

4. ROLES & RESPONSIBILITIES



The Business Heads, safety teams, maintenance teams, and others open to risks are the major places where risks can be identified in an organization. The identified risks are reported to the Internal Management Committee who have to record these risks, inform the Risk Management Committee, Audit Committee and Board of Directors and make decisions regarding how to handle the particular risks. The Role Mapping is shown in the above diagram. The responsibilities are explained in details below.

4.1 Business Heads & Others

The responsibilities of the Business Heads, Safety Teams, Maintenance Teams, and Others are:

1. Identify all types of possible risks in the Business by brainstorming or other procedures
2. Suggest ways to reduce or mitigate the identified risks
3. Report the effect of changes in the dynamic business environment

4.2 Internal Management Committee

The Internal Management Committee comprises of the Senior Management Team.

The responsibilities of the Internal Management Committee are:

1. Aggregate all risks, try to use other techniques/ external consultants to address all relevant risks and record them in the risk register
2. Assess and evaluate each risk and record it in the risk register, identify all ways to mitigate/ reduce the risk
3. Report the risk to people higher in the value chain (Risk Management Committee, Audit Committee, & Board of Directors) and make decision on how to handle the risks (retain/reduce/transfer/share, etc)
4. Record the mitigation plan on the Risk register, reassess and evaluate the risk, and be in line with the changes in the dynamic environment
5. All the Risks are reviewed and checked at regular intervals, at least yearly once, and if there are any other major dynamic changes.

4.3 Risk Management Committee

The Risk Management Committee has members as constituted by the Board from time to time.

The responsibilities of the Risk Management Committee are:

1. Suggest missed-out risks to the Internal Management Committee & Review all the risk related data
2. Suggest Mitigation plans to the Internal Management Committee
3. Make decision on how to handle/ treat the risks based on a cost-benefit analysis, report this information on the risk register and set the Threshold Limits
4. Seek external advice from Experts if required

4.4 Audit Committee

The responsibilities of the Audit Committee are:

1. Review the Risk Reports, Policies, Mitigation Plans, Analyses & suggest improvements

4.5 Board of Directors

The responsibilities of the Board of Directors are:

1. Review the Risk Reports, Policies, Mitigation Plans, Analyses & suggest improvements

5. REFERENCES

ISO 31000 2009 Risk Management Dictionary:
http://www.praxiom.com/iso-31000-terms.htm

The Risk Management Standard, Institute of Risk Management, UK:
https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

ANNEX-1

S. No.	Risk Type	Risk Name	Description
1	Business	Markets/ Customer	Economic Crisis/ Declining Economic growth/ Black-swan Declining total markets or specific market segments Increased Competition Negative impact of Pricing arrangement Loss of Accounts Receivable/ Defaults
2	Strategic	Production & Technology	Research & Development Risks Quality Risks Risks from Warranty & Policy Production Utilization/ Capacity
3	Strategic	IT	Timeout & Cost overrun IT Security Insufficient (unauthorized access, viruses) Disaster Recovery Plan Unintegrated software solution, lack of compatibility System stability Physical Hardware safety, standards for fire, power outage
4	Strategic	Human Resource	Lack of right personnel Motivation risks Succession Planning Work safety Loss of labor (eg: employee illness, strike) Increasing personnel costs
5	Operations	Financial Market	Exchange Rate Risk Interest Rate Risk Credit Risk, Liquidity and Indebtedness Risks Risks from Capital Markets Risks from Portfolio Realignments Capital availability and allocation Rating/ Requirements of stake-holders
6	Operations	Supply Market	Keeping/ meeting Quality Standards Supply Constraints Meeting efficiency targets/ purchasing budget Insolvency of suppliers Reliability of Suppliers (in terms of quality, etc)
7	Regulatory Environment	Legal & Political Environment	Risks of the Political & Social system Violation of law, legal requirements and regulations (eg: protection of environment) Product Liability Risks from Warranty/ Policy Tax increases Risks from class actions

S. No.	Risk Type	Risk Name	Description
8	Societal	Disastrous	Natural Disasters (earthquake, hail, tsunami, flooding) Explosions, fires Terrorist Attacks War/ strikes, riots and civil commotions
9	All	Others	Restructuring changes Organizational Risks (Business Model, Portfolio, Organization Structure) Risks of evaluation and assessment Intellectual Property Risk

ANNEX-2

Risk Register																			
Risk Identification					Risk Assessment & Evaluation						Risk Handling								Risk Monitoring
Risk ID	Raiser	Date Registered	Classification	Description	Prob.	Impact	Score	Change	Last Reviewed	Risk Proximity	Response Category	Response Plan	Trigger	Owner	Total Cost	Total Benefits	Prob.	Impact	Score	Status
					High	High				Imminent	Mitigate						High	High		Open
					Medium	Medium				Long-Term	Share						Medium	Medium		Close
					Low	Low				Short-Term	Avoid						Low	Low		
											Accept									
											Others									