Risk Management Policy

November 2015

Contents

A. Risk Management Policy

1 Overview

1. The company recognizes that risk is inherent to any business activity and that managing risk effectively is critical to the immediate and future success of the Company.
2. The Company, through this Risk Management Policy, presents an enterprise-wide approach to ensure that key aspects of risk that have an enterprise-wide impact are considered in its conduct of business.
3. This policy document serves as a guideline for respective components of risk which have a common resonance across the company.
4. Risk Management in the Company provides a framework to identify, assess and manage potential risks and opportunities. It provides a way for managers to make informed management decisions
5. The Risk Management Policy provides entity level risk guidelines encompassing key risk areas across the group such as Business Risk, Operational Risk, technology risk and Strategic and Reputation risk.

Scope

6. The Policy shall apply to all operations, divisions and geographic locations of the Company
7. The Policy shall also apply to all Indian and International Subsidiaries.

Terms and Definitions

8. Terms and definition are included in Annexure for reference

Components of a Sound Risk Management System

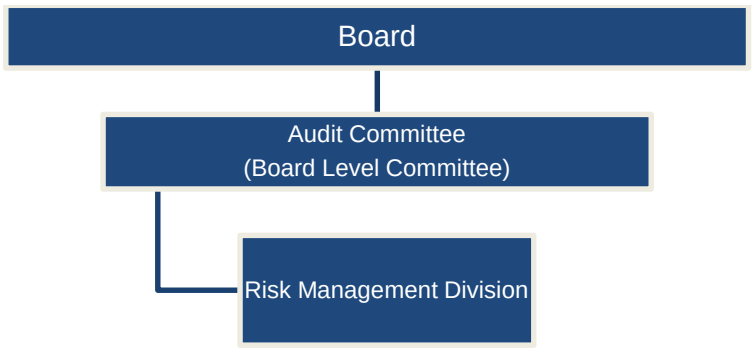
9. The risk management system at the Company has the following key features:
    - Active board and senior management oversight
    - Appropriate policies, procedures and limits
    - Comprehensive and timely identification, measurement, mitigation, controlling, monitoring and reporting of risks
    - Appropriate management information systems (MIS) at the business level
    - Comprehensive internal controls in accordance with current regulations
    - A Risk Culture and communication

Risk Management Principles

10. The principles contained in this policy and strategy will be applied at both corporate and operational levels within the organization.
11. The Company's Risk Management Policy and Strategy will be applied to all operational aspects of the Company.
12. Our positive approach to risk management means that we will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalizing on corporate strengths
13. Responsibility for identifying and managing risks is a routine part of the role of management at all levels, including the identification and regular monitoring of key risk indicators;

2 Risk Governance

14. An organisation's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities.
15. Risk governance signifies the manner in which the business and affairs of an entity are directed and managed by its Board of Directors and executive management.
16. The risk organization structure for the Company is as depicted below.



2.1 Roles and Responsibilities

Board	The Company's risk management architecture is overseen by the Board of Directors (BOD) and policies to manage risks are approved by the Board • Ensure that the organization has proper risk management framework • Define the risk strategy and risk appetite for the company • Approve various risk management policies including the code of conduct and ethics • Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks
Audit Committee	The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control, and c) compliance with laws, regulations, and ethics (d) financial and risk management policies. • Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; • Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies. • Ensure that senior management monitors the effectiveness of internal control system • Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.
Risk Management Function	The Risk Management Division is the key division which would implement and coordinate the risk function as outlined in this policy on an ongoing basis. It would act as the central resource division for administration of RMF • Developing and communicating organizational policy and information about the risk management programme to all staff, and where appropriate to our associates / suppliers / contractors etc.; • Develop, enhance and implement appropriate risk management policies, procedures and systems • Work with risk owners to ensure that the risk management processes are implemented in accordance with agreed risk management policy and strategy • Review risks and risk ratings of each department

	• Collate and review all risk registers for consistency and completeness • Provide advice and tools to staff, management, the Executive and Board on risk management issues within the organisation, including facilitating workshops in risk identification • Oversee and update organisational-wide risk profiles, with input from risk owners
Business Units	• Comply with Company standards which relate to particular types of risks; • Manage the risk they have accountability for • review the risk on a regular basis • identify where current control deficiencies may exist;

3 Risk Management Framework

3.1 Risk Appetite

17. The Board shall approve the risk profile or appetite of the Company in material risk areas. The objective of risk appetite statements is to restrict the overall risk levels of the Company based on pre-defined strategies.
18. Risk appetite is communicated through the Company's strategic plans. The Board and management monitor the risk appetite of the Company relative to the Company's actual results to ensure an appropriate level of risk tolerance throughout the Company
19. Risk Manager shall develop the Risk Appetite statements and submit to the Board for review and approval.
20. Risk Appetite statements shall be reviewed annually for necessary changes. Any breach of the appetite statements shall be reported to the Board at the next meeting.

3.2 Risk identification

21. Risk identification forms the core of the Risk Management system. Multiple approaches for risk identification are applied to ensure a comprehensive Risk Identification process.
22. The company shall identify sources of risk, areas of impacts, events and their causes with potential consequences. Comprehensive identification is critical, because a risk that is not identified here will be missed from further analysis.

3.3 Risk Assessment and Risk Rating

23. For all key risks identified during the Risk Identification process, a qualitative and quantitative assessment is carried out.

24. Risk assessment involves different means by which to grade risks in order to assess the possibility of their occurrence and extent of damage their occurrence might cause.
25. Likelihood rating and impact rating is as per the Rating parameters defined by the Company.

3.4 Risk Prioritization

26. After the risk assessment is complete, it is the responsibility of the Risk Management Function to prioritize the key risks to determine which risk are considered key and need to be addressed on a priority basis.
27. Prioritization of risks involves using final ratings. The risks are plotted on a 3X 3 matrix, to identify which risks are materials from a corporate perspective.
28. For this purpose, the materiality scales are used to identify the severity and likelihood of these risks.
29. All risks that fall in the red zone are considered high risk and require immediate attention in terms of risk management.
30. The findings of risk prioritization are presented to Senior Management and Business Units.

3.5 Risk Mitigation Process

31. Once the top or critical risks are prioritized, appropriate risk mitigation and management efforts to effectively manage these risks are identified.
32. Risk mitigation strategy usually involves identifying a range of options for treating risk, assessing those options, preparing and implementing risk treatment plans. The risk mitigation strategies may include managing the risk through implementation of new internal controls, accepting certain risks, taking insurance, and finally avoiding certain activities that result in unacceptable risks.
33. Proposed actions to eliminate, reduce or manage each material risk will be considered and agreed as part of the Risk Assessment Workshops or as part of Management/Risk Committee.

3.6 Risk Reporting and Monitoring

34. An enterprise-wide integrated Risk Management Information System (MIS) needs to be implemented by the company.
35. 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.

3.7 Action Plan and Status

36. A risk mitigation action plan is outlined for all priority risks in the high and medium categories. Senior Management and Business Heads design an action plan to mitigate and monitor each of these key risks.
37. An action plan and status reporting is implemented to log actions proposed to mitigate risks and track status of Evidence, of regular review and monitoring of the profile and action plan.
38. The action plan and status reporting is reported quarterly to Audit/Risk Committee to update on the status of mitigation efforts.

3.8 Internal Controls and Risk Management

39. Individual Business Units are responsible, along with support from Risk Management and other support functions, for establishing effective internal controls within various business processes. Effective design and implementation of the internal control framework is validated by regular internal audits and test of controls for these units.

3.9 Review of Risk Management Policy

40. The Risk Manager shall have the ownership of the Risk Management Policy and shall be responsible for implementation of the policy aspects. The policy document shall be reviewed and approved by Audit Committee.

B. Risk Management Processes

4 Risk Identification Process

1. The risk identification process should capture all significant risks and identify potential threats facing the organisation.
2. Risk Identification is performed at strategic functions at the entity level as well as at the process level for each function and process.

4.1.1 Business Functions

1. For the purpose of risk identification and to ensure that all risks across each business are captured, the Company's operations are divided into Business Functions and major processes as outlined in Annexure 1

4.1.2 Risk Register

1. For the purpose of consolidation of material risks, all the outputs of the various risk identification and assessment processes are reviewed by the Risk Manager in collaboration with Business Heads. These are aggregated in a Risk Register capturing the key risk, mitigating controls and other details about the particular risk.
3. A Risk Register is to be maintained by the company in the prescribed format which contains a listing of all the risks identified by the company.
4. Certain risks will already be a part of the IFC Framework as part of risk impact internal controls. Accordingly, the Risk Register shall be a repository of top Enterprise level risks that are broader and more macro level that require mitigation.

4.1.3 Maintenance and regular Updates

1. Risk Manager shall coordinate and maintain the Risk Register and ensure that it is current at all times.
2. For this purpose, informal interactions with Departmental Heads are likely to identify new or emerging risks that are considered key.
3. Business Heads are the owner of the risk register and shall update risks in the risk register for the department and forwards to the Risk Manager.
4. These are updated by the Risk Manager into the consolidated Master Risk Register on a continuous basis.

4.1.4 Periodic Risk Assessment Workshop

1. In addition, a formal risk identification process, as outlined above, in the form of a workshop or similar methodology, is performed half yearly to review and revise the Risk Register. For this purpose, Senior Management and Departmental Heads are engaged in an active dialogue to discuss these risks.

2. Revised Risk Register is circulated for final approval, once other risk management steps have been completed.

4.1.5 Incident Reporting / Loss Incidents

1. Incident / Loss reporting occurs as part of day to day business that requires escalation of major events having financial or reputation impact.
2. Such events with significant risks shall be reported by the different businesses and functions on a regular basis to understand the adequacy of the risk management activity and evaluate the effectiveness of the processes.
3. The process requires all functional units to report all kinds of events which are unusual in nature and occurring in their daily course of activities.
4. Incident Reporting shall be done via email to Risk Management Function explaining the event in details along with event date, likely financial loss, mitigation actions taken and other necessary details
5. Risk Management Function shall maintain a log of major incidents reported and also present a summary of major incidents to Audit Committee on a regular basis.

5 Risk Assessment Process

1. Risk Assessment and rating methodologies take a systematic approach to determine the impact of occurrence of a risk and its likelihood of happening. In brief, the assessment involves following key steps
   - Rating of each risk as per the probability of the risk event occurring
   - Rating the risk as per the financial impact of that risk event should the risk event occur. The two parameters provide the quantitative element to risk assessment.
2. Risk Rating scales adopted by the Company are included as Annexure 2
3. The process of Risk Assessment shall cover the following:
   a) **Risk Identification and Categorisation** – the process of identifying the company's exposure to uncertainty classified as Strategic / Business / Operational.
   b) **Risk Description** – the method of systematically capturing and recording the company's identified risks in a structured format
   c) **Risk Estimation** – the process for estimating the cost of likely impact either by quantitative, semi-quantitative or qualitative approach.
4. Once the risks are analysed, these can be plotted on a heat map and shared with the Audit Committee.

5. As part of the above risk assessment, key risks falling in the red zone will be subject to greater risk management by way of monitoring and mitigating controls.
6. Accordingly, risks with a residual risk rating score of 6+ are considered significant risks which require risk mitigation on a priority basis

6 Risk Monitoring and Risk Reporting

6.1 Risk Monitoring

1. The risks are to be monitored and treated by the Risk team under the guidance of Risk owner on a frequent basis. The risk owner reviews all the risks identified and profiled on quarterly basis with reference to the risk mitigation plan.
2. A risk mitigation action plan is outlined for all priority risks in the high and medium categories. Senior Management and Business Heads design an action plan to mitigate and monitor each of these key risks.
3. An action plan and status reporting is implemented to log actions proposed to mitigate risks and track status of Evidence, of regular review and monitoring of the profile and action plan. The action plan and status reporting is circulated quarterly to stakeholders to update on the status of mitigation efforts.
4. The Company shall also introduce some high level Key Risk Indicators that will provide leading and lagging indicators on some key risks.

6.2 Risk Reporting

1. The Company's MIS provides the Board and senior management in clear and concise manner timely and relevant information concerning the risk profile. The MIS is capable of capturing major policy breaches and effective in promptly reporting such breaches to senior management, as well as to ensure that appropriate follow-up actions are taken.
2. Most of the internal reporting and day to day interactions between senior management and Business Functions ensures that senior management is aware of key risks and unusual incidents or loss events.
3. In addition to this, formal risk reporting has been introduced to highlight risk profiles, trends, key issues and effectiveness of Risk Management Systems.
4. The ongoing business success of the Company depends to a great extent on risk awareness and the ability to manage risks. This requires transparency of all risk taking activities and thus an effective risk reporting system.

5. The following is a summary of the Risk Management Reporting that communicates the risk profile and risk mitigation efforts.

a) Company and Business Risk Profile

In order to manage risks, key risk dashboards are implemented to review risk levels at a Company level as well as at business function levels.

b) Risk Monitoring and Risk Calendar

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the updation of the Risk Matrix will be done on a regular basis.

The Risk Manager shall maintain a risk calendar that outlines the frequency of performance of various risk management activities. The risk calendar is attached as Annexure -3

Quarterly Review of Risk Management Framework

Progress on implementation of Risk management system is reviewed by the Audit Committee on a quarterly basis and submitted to the Board as part of the Board Reporting Package.

7 Other aspects relating to Risk Management

7.1 Other Risk Related Policies

1. The Company has implemented other risk management related policies separately for areas that require comprehensive risk identification and implementation. These policies are

    - Fraud Risk Management Policy
    - Investment Policy with FX Risk Management Policy
    - Compliance Policy
    - IFC Framework

7.2 Integration of Audit and Risk Management

2. Internal control is broadly defined as a process, implemented by the Board of Directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

3. Individual Business Units are responsible, along with support from Risk Management and other support functions, for establishing effective internal controls within various business processes. Effective design and implementation of the internal control framework is validated by regular internal audits and test of controls for these units.

4. The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the Company to respond to a variety of operational, financial, and commercial risks. These elements include:

Policies and procedures

Policies and procedures are the foundation for an effective internal control framework that then supports a strong risk management framework. Written procedures support the policies where appropriate.

Business planning and budgeting

The business planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting business plan objectives is monitored regularly.

Independent Internal Audit function

A risk based internal audit approach is adopted by the company to ensure adequacy and effectiveness of internal control and policy framework.

Audit Committee.

The Audit Committee is required to report to the Board on internal controls, and to alert it of any emerging issues. The committee is therefore well placed to provide advice to the Board on the effectiveness of the internal control system, including the Company's system for the management of risk.
Detailed Internal Control over Financial reporting forms part of the "Internal Control Systems and Controls" policy.

7.3 Risk Management requirement as per Clause 49

1. This policy is in compliance with clause 49 of Listing Agreement, which requires the Company to lay down procedures about the risk assessment and risk management.

2. The Board of Directors of the Company and the Audit Committee of Directors shall periodically review the risk management policy of the Company so that management controls the risk through properly defined network.
3. Head of Departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the Board and the Audit Committee.

7.4 Risk Management Culture, Training and Awareness

1. To realise return on risk, senior management needs to ensure risk awareness is embedded into the organisation culture. This includes its consideration in key decisions, preparedness among staff to take ownership of risk within their operations and ultimately the development of integrated metrics (a common 'language') that seek to align risk and performance management across the business
2. All employees should have a clear understanding of their risk management responsibilities and be held accountable for their performance in that respect.
3. Periodic risk management training is imparted to company employees and senior management to inculcate a uniform risk management culture. Targeted trainings on specific topics are undertaken by select employees based on their role in the Risk Management Framework.

7.5 Adequacy of Insurance

4. On an annual basis, along with key Business Heads, performs an annual review of Insurance Policies to evaluate the existing insurance policies for adequacy of coverage, identification of key risks covered by these policies, compliance of policies.
5. Insurance cover adequacy is reviewed taking into consideration historical events and proposed business growth. Any significant gaps in terms of shortfall of insurance will be reviewed with Senior Management and additional coverage proposed.
6. On completion of the insurance review, key findings are summarized and reported to Senior Management. Action points / Issues arising from this reporting, if any, are noted and followed up.

8 Annexure 1: Business Lines

Business Department	Major Process
Accounting	Intercompany
	International Accounts
	Prepaid Expenses
	SAP Masters
	Share capital and reserves and surplus
	Cash and Bank
Administration	Administration
	Procurement
Corporate	Governance
	Projects
	Strategy
	Corporate Communication
Compliance	Secretarial
	Legal Department
Finance	Investments & Treasury
	Loans and Borrowings
	Taxation
HR	Compensation & Benefits
	Hiring & on boarding
	Training
	Payroll Processing
IT	Applications
	IT Infrastructure
Logistics	Depots & Warehouses
	CNF
	Logistics
Marketing	Marketing
	Business Development
Purchases	Purchases
	Supply Chain
	Vendor Setup
Production & Factories	Material Management
	Manufacturing & Maintenance
	Inventory

9 Annexure 2: Risk Assessment Parameters / Rating Scales

IMPACT RATING PARAMETER

Impact	Comments	Minor	Moderate	Major
		1	2	3
Financial	Loss	Upto Rs 5 Lac	Rs 5- Rs 50L	Rs 50L+
Reputation	Letters to local/industry press/ investor confidence/extensiveness of negativity	Series of articles or complaints in press or by customers/ business associates/ stakeholders	Extended negative local/industry coverage & short term disruption to confidence level of customers/ business associates	Extensive negative media coverage and disruption to confidence level of customers/ business associates/ stakeholders
Regulatory	Minor/penalties to business closure	Minor penalties	Major penalties	Major Censure
Business Disruption		Business disruption leading to minor business losses. One-off and/or short term disruption at the individual unit level. Middle level management required.	Business disruption leading to moderate business losses. Medium term business disruption at the business level. Business head effort required.	Business disruption leading to major business losses. Sustained period of disruption at the organisational level. Significant senior management effort required.

LIKELIHOOD RATING PARAMETER

Likelihood	Unlikely	Likely	Highly Likely
	0-15%	15-65%	>65%
	1	2	3
	Event could occur at some time, although unlikely	Event will probably occur	Event is expected to occur in most circumstances

10 Annexure 3: Risk Calendar

Risk Management Activity	Responsible Person	Details and Audience / Reporting To
Regularly / As needed		
Updates to Current Action Plan	Department Head	Execute action items identified in the Action Plan. Review current Action Plan and update the Action Plan details regularly for providing periodic updates to Risk Division.
Monthly		
Updates to Current Action Plan	Risk Manager	Review of current Action Plan and take updates from each Business Function and update the Action Plan column of Risk Register on a monthly basis.
Quarterly		
Risk Heat Maps	Risk Manager	Develop Departmental heat maps and reports as Risk Dashboard to Audit Committee.
Summary of Incidents Occurred	Risk Manager	Compile a summary of risk / loss incidents occurred during the period and present to Management Committee.
Half Yearly		
Review of Risk Register	Risk Manager	Updates to Risk Register and sharing updated risk register with Business Functions and Audit Committee
Annually		
Review and revision to Risk Management Policy	Risk Manager / Audit Committee	Review of Risk Management Policy and update as necessary. Updated Risk Management Policy to be reviewed and approved by Audit Committee
Review of Risk Appetite	Risk Manager / Audit Committee	Review of Risk Appetite Statements. Risk Appetites shall then be placed to Board for approval.

11 Annexure 4: Terms and Definition

Risk
Risk is often described by an event, a change in circumstances or a consequence that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. Thus, risk is the effect of uncertainty on objectives.

Risk Management
Risk Management is the coordinated activities to direct and control an organization with regard to risk. It is the process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

Risk Management Policy
Risk Management Policy is a statement of the overall intentions and direction of an organization related to Risk Management.

Risk Management Framework
Risk Management Framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving Risk Management throughout the organization.

Risk Management Plan
Risk Management Plan is a scheme or an operation plan within the Risk Management Framework specifying the approach, management components and resources to be applied to management of risk.

Risk Strategy
The Risk Strategy of an organization defines its readiness towards dealing with various risks associated with the business. It describes the organization's risk appetite or tolerance levels and decision to transfer, reduce or retain the risks associated with the business.

Risk Owner
Risk Owner is a person or entity with the accountability and authority to manage risk.

Risk Assessment
Risk Assessment is defined as the overall process of risk identification, risk analysis and risk evaluation.

Risk Estimation
Risk Estimation is the process of carrying out quantitative, semi-quantitative or qualitative assessment of risk in terms of the probability of occurrence and the possible consequence.

Risk Identification
Risk Identification is a process of finding, recognizing and describing risks.

Risk Source
Risk Source is an element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Tolerance / Risk Appetite

Risk Tolerance or Risk Appetite is a driver of Risk Strategy of an organization. It defines the maximum quantum of risk which the company is willing to take as determined from time to time in consonance with the Risk Strategy of the company.

Risk Description
A Risk Description is a comprehensive template covering a range of information about a particular risk that may need to be recorded in a structured manner. It is an input to the Risk Register.

Risk Register
A 'Risk Register' is a tool for recording risks encountered at various locations and levels in a standardized format of Risk Description. It becomes a major input in formulating subsequent Risk Strategy.

Likelihood
Likelihood means the chance of something happening; whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively and described using general terms or mathematically such as a probability or a frequency over a given time Period.

Risk Profile
Risk Profile is a description of any set of risks that may relate to the whole or part of the organization or as otherwise defined.

Risk Analysis
Risk Analysis is a process to comprehend the nature of risk and to determine the level of risk. It provides the basis for Risk Evaluation and decisions about Risk Treatment and includes Risk Estimation.

Risk Criteria
Risk Criteria is a terms of reference against which the significance of a risk is evaluated. They are based on organizational objectives and external or internal context and can be derived from standards, laws, policies and other requirements.

Risk Evaluation
Risk Evaluation is a process of comparing results of Risk Analysis with Risk Criteria to determine whether the risk and / or its magnitude is acceptable or tolerable. It assists in the decision about Risk Treatment.

Risk Treatment
Risk Treatment is a process to modify a Risk. It that deals with negative consequences is also referred to as 'Risk Mitigation', 'Risk Elimination', 'Risk Prevention' and 'Risk Reduction'. It can create new risks or modify existing Risks.

Control
Control is a measure of modifying risk and includes any process, policy, device, practice or other actions which modify risk. It may not always exert the intended or assumed modifying effect.

Residual Risk
Residual Risk is a risk remaining after Risk Treatment. It can contain unidentified risk and also be known as 'Retained Risk'.

Version Control

S. No.	Rev. No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for New Release
1	1	November 2015	Riskpro India	Sujit Shetty		Initial Draft