ENTERPRISE RISK MANAGEMENT

POLICY

OF

AIROX TECHNOLOGIES LIMITED

Table of contents

1. Overview

Pursuant to Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("**SEBI Listing Regulations**") and Section 134(3) of the Companies Act, 2013, Airox Risk Assessment and Management Policy ("**ARM Policy**") establishes the philosophy of Airox Technologies Limited ("**Company**"), towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company. This ARM Policy is applicable to all the functions, departments and geographical locations of the Company.

Each business operates in dynamic environment & given the markets, growth & structure, elements of risk are inherent. The board of directors of Company ("**Board**") should recognize the importance of identifying and controlling risks and to ensure that required internal controls and procedures have been established which are designed to safeguard assets and interests of the company, and to ensure the integrity of reporting. Accordingly, the Board has adopted this ARM Policy at its meeting held on 20th May, 2022 which can be amended from time to time.

The purpose of this Policy is to

- Facilitate proactive risk management
- Enhance understanding of all risks faced by the business
- Facilitate the prioritization of risks
- Enhance the effectiveness of risk management activities

This will allow the Company to make better business decisions through focus on risk & return which in turn will enhance the value for the business & preserve its soundness & profitability overtime. Enterprise Risk Management (ERM) deals with risks and opportunities affecting value creation or preservation & takes a broad perspective on identifying the risks that could cause an organization to fail to meets its strategies & objectives.

ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives**.**

Policy Statement

ARM Policy is to achieve best practice in the management of all risks that threaten to adversely impact the business, its customers, people, assets, functions, objectives, operations or members of the public. Risk Management will form part of corporate strategies, operational and line management responsibilities of Airox Technologies Limited and be integrated into the strategic and business planning processes. Risk Management ensure the following:

i. Implementation and documentation or risk management procedures and guidelines, adherence to Risk Management Standards.
ii. Compliance with regulatory requirements and guidelines
iii. Identification of risks and successful treatment in accordance with procedures and guidelines,

iv. Mitigation and control of any losses,
v. Monitoring and reporting of risk to Board of Directors and Senior Management, and
vi. Achievement of best practice.

Every employee of Airox Technologies Limited is recognized as having a role in the risk management vigilance in the identification of risks to treatment and shall be invited and encouraged to participate in that process. The defined Policy and objectives will be applicable at the enterprise level and effectiveness of our risk management will be determined based on our performance results

2. Objective

Key objectives of this Policy are to:

- Endorse a structured approach to identify current and future potential risks to organization.
- Mandate an ERM framework
- To establish and maintain a system of internal controls to promote effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.
- Mandate the allocation of each risk to a risk category so that appropriate governance structures and policies & procedures can be developed and implemented.
- Facilitate the making of informed decisions including the prioritization of identified risks
- To facilitate the monitoring and reporting on status of all risks to the risk committee & Board of Directors.
- Provide reasonable assurance with respect to organization's ability to achieve its strategic and business objectives.

3. Policy Guidelines & Principles

These guidelines recognize that the activities undertaken by organization with respect to the achievement of its strategies and business objectives are ultimately tied to decisions about the nature and level of risk it is prepared to take and the most effective means to manage and mitigate those risks. This ERM provides policies and procedures for risk management and internal control to be laid down for Airox Technologies Limited.

The ERM framework which shall govern the related management policies and procedures shall be premised upon common understanding and application of following principles:

- The informed acceptance of risk is an essential element of good business strategy.
- Risk management is an effective means to enhance and protect the value of business overtime.
- A common definition and understanding of risks are necessary, in order to better manage those risks and make more consistent and in formed business decisions.
- The management of enterprise risk is an anticipatory, proactive process, to be embedded in corporate culture and a key part of strategic planning & operational management.

- All risks are to be identified, assessed, measured, managed, monitored and reported on in accordance with management policies and procedures.
- All business activities are to adhere to risk management practices which reflect effective internal controls that are appropriate for business.

The principles on which this Policy document is based and the guidelines set out herein shall be reviewed periodically to ensure that they remain appropriate, in light of changing circumstances and to ensure that such principles and policies are effectively implemented.

4. ERM Policy Parameters

The ERM framework in place for Airox Technologies Limited shall be based on following Policy parameters:

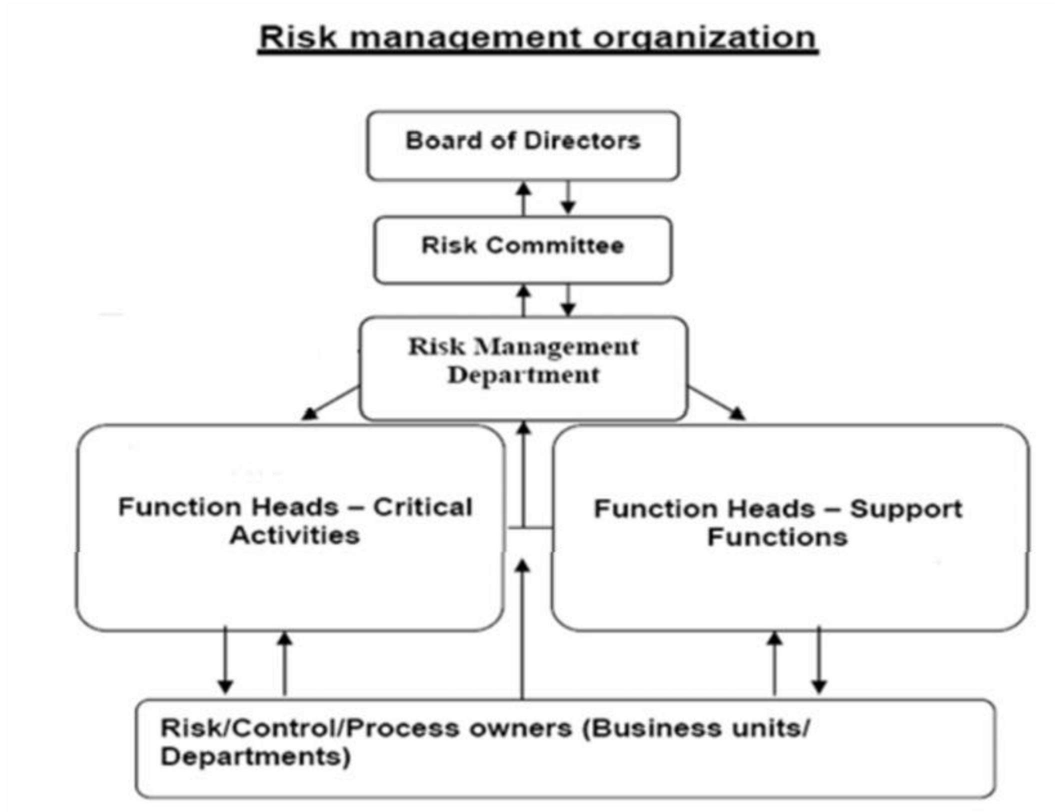
- The nature and level of risks assumed, risk categories into which risks are grouped within ERM framework to be based on respective business activities
- We have to develop comprehensive, integrated management policies and procedures that, taken together will apply to its significant activities, which shall be based on risk management objective, and governance structure
- We are responsible for risk management within the domain of our business area and also for ensuring that appropriate practices and internal controls are in place and are being followed in order to manage any risk event associated exclusively with the line of our business.
- ERM framework to be approved by Board should focus on risk, being any catastrophic or significant risk that can originate in any part of business, which when viewed from enterprise-wide perspective, could potentially cause business to fail to achieve its strategic goals & objectives.

All risks to be identified and assessed appropriately based on enterprise wide practices.

- ERM framework should specify risk response mechanisms. Each risk to be evaluated toconfirmappropriateresponsetomitigatesuchrisk.Agreeduponriskresponsesmayinclud e:
  1. Establishment of risk mitigation controls and action plans
  2. Sharing of risk with third parties including insurers
  3. Acceptance of risk
  4. Adoption of other risk avoidance measures.
- Risk responses should be directed by Board of Directors, Risk management committees & Senior Management and put into effect by ERM functions. Risk response as implemented to be reviewed, evaluated and confirmed from time to time by senior management.
- All risks should be assessed at the inherent levels (processes without controls) and the residual level (processes with existing control), which will help to assess the effectiveness of controls and gaps if any.

5. Risk Organization

A robust organizational structure for managing and reporting on risks is a pre-requisite for an effective risk management process.



6. Roles and Responsibilities

i. Role of Board of Directors

The Company's Board of Directors has the responsibility for overseeing all risks associated with the activities of business, establish a strong internal control environment and risk framework that fulfills the expectations of stakeholders of business.

The Board of Directors will review this Policy statement on an annual basis, or sooner, depending on the circumstances facing the organization.

ii. Role of Risk Management Committee:

The Risk Management Committee provides an overall assessment of risks impacting the activities of the company and should meet on periodic (quarterly) basis or whenever events warrant. The Risk Management Committee is responsible for the following activities:

- The Risk Management Committee would monitor on overall process of evaluation and assessment, progress of evaluation of control effectiveness, key control deficiencies observed and counter measures to address these. Monitoring would also include significant changes in assessment of key risks or new risks identified if any.
- Review and approve modifications to existing policies, procedures, and overall risk management framework comprehensive review of this Policy document on an annual basis.

- Composition of the Risk Management Committee will be as per the requirement setout in appropriate statute.

iii. Role of Chief Risk Officer

Chief Risk Officer has overall responsibility for the development and implementation of risk control principles, frameworks, and processes across all categories of risks faced by organization. A key responsibility of Chief Risk Officer includes:

- Providing the overall leadership, vision and direction for enterprise risk management;
- Establishing an integrated risk management framework for all aspects of risks across organization.
- Developing risk management policies and review of the same Ensuring effective information systems exists to facilitate overall risk management within institution
- Developing the analytical systems and data management capabilities to support risk management

Clear objectives and key performance indicators should be set for Chief Risk Officer. These indicators must be able to measure the Chief Risk Officer effectiveness in leading institution's ERM framework.

iv. Role of Function Heads and Risk and Control Owners

Risk and Control Owners are the personnel who are best placed to influence and manage the risk/ control or are best placed to report on the risk/ control. On an ongoing basis, Risk and Control Owners monitor their areas for new risks/events or assess changes in risk exposure; as well as carryout periodic assessment of controls in line with the above and report on the same.

Specifically risk and control owners with in business units and departments are responsible for:
- Ongoing identification and evaluation of risks within the business and operations;
- Selecting and implementing risk measures on a day to day basis; if any
- Managing certain specified risks under the guidance of the Risk Committee;
- Reviewing the effectiveness, efficiency and suitability of the risk management process and addressing weaknesses;
- Maintaining efficient and cost-effective risk handling mechanisms or control framework in line with changes in the business.

7. Risk Management Process

Risk management is continuous interplay of actions that permeate the company. It is affected by Board of Directors, senior management and other personnel. The risk management process of the company aims at providing reasonable assurance regarding achievement of company's objectives.

In order to provide reasonable assurance, the Company's risk management process endeavors to help:

- Identify, assess and escalate new risks impacting the objectives of the Company,

- Define measures to respond to the new risks effectively,
- Monitor movement (if any) in existing risks,
- Monitor effectiveness of existing risk management measures, and
- Report risks and risk management measures to the Risk Management Committee

The processes mentioned above are in the sequence followed, for performing risk management for the first time, and should not be followed strictly in a serial process for risk management on a non going basis. Risk Management is a dynamic process and almost any component can and will influence another and hence risk processes can change/alter with changing market dynamics.

i. Risk Identification

- The risk management process starts with the systematic identification of risks. Only if such risks are recognized in a timely manner can they be successfully managed.
- A prerequisite for efficient risk identification and subsequent risk treatment is a consistent and comprehensive understanding of business objectives and strategies. There could be other risks which will emanate because of changes in the internal or external environment within which business operates. These risks are to be identified by the Risk Owners during the normal course of business

ii. Risk Assessment

- Once risks are identified, they are appropriately assessed based on enterprise wide practices
- Each risk might get assessed based on impact (materiality of the risk if it occurs) and likelihood (at an agreed level of impact, the probability of the event taking place). Reporting to the Risk Committee should be as follows:
  - Reporting of significant events /incidents should be done as and when they occur
  - Reporting on the changes in the Risk profile on a quarterly basis. Risks would be updated i.e. added, deleted and reassessed.
- 'Process Owners' and 'Function Heads' would be responsible to Self-Assess and report any exceptions to the Enterprise Risk Management team.

iii. Developing Risk Response and Assessing Control Activities

Thethirdstageoftheriskmanagementprocessisriskresponsehandling.Managementselectsaseries oftoreducethepotentialimpactoftheriskshoulditoccur

Possible responses to risk include avoiding, accepting, reducing or sharing the risks.

Risk Mitigation Plan

The Board to develop appropriate responsive action on review of various alternatives, costs and benefits, with a view to managing identified risks and limiting the impact to tolerance level. Risk mitigation plan drives Policy development as regards risk ownership, control environment timelines, standard operating procedure, etc.

Risk mitigation plan is the core of effective risk management. The mitigation plan covers: (i)Required action(s); (ii) Required resources; (iii) Responsibilities; (iv) Timing; (v) Performance measures; and (vi) Reporting and monitoring requirements The mitigation plan also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; (iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident. Therefore, it is drawn with adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risk events.

Risk avoidance
Withdrawal from activities where additional risk handling is not cost effective and there turns are unattractive in relation to the risks faced.

Risk acceptance
Acceptance of risk but the potential returns are attractive in relation to the risks faced.

Conflict in Policy
In the event of any conflict between the Companies Act or the SEBI regulations or any other statutory enactments ("**Regulations**") and the provisions of this Policy, the Regulations shall prevail over this Policy.

Risk reduction
Activities and measures designed to reduce the probability of risk crystallizing and/or minimize the severity of its impact should it crystallize (e.g. hedging, reinsurance, loss prevention, crisis management, business continuity planning, quality management).

Risk sharing
Activities and measures designed to transfer to a third-party responsibility for managing risk and/or liability for the financial consequence of risk should it crystallize.

In accordance with the defined roles and responsibilities, the operating departments are responsible for implementing sufficient risk handling to manage risks at an acceptable level. If necessary, guidance on the development and implementation of risk handling measures may be attained from the Risk Committee.

iv. Monitoring Risk and Controls

There need to be adequate controls and ongoing monitoring mechanisms to enable timely notification of fundamental changes in risks or their handling measures. Since the internal and external environment within which the Company operates is exposed to change continuously, the risk management process must remain sufficiently flexible to accommodate new situations as they arise. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change.

In the face of such changes, management needs to determine whether the functioning of the risk management framework continues to be effective. Ongoing monitoring by the Risk Owners, and the Risk Committee to be done in following way:

- **Risk and Control Owners** are responsible for monitoring risks and effectiveness of their counter measures. They are also responsible for the development and implementation of risk management action plans.

- **The Risk Committee** is responsible for monitoring adherence to the risk policy and guidelines and reviewing the overall risk management system in light of changes in external and internal environment within which the Company operates.

v. Risk Reporting

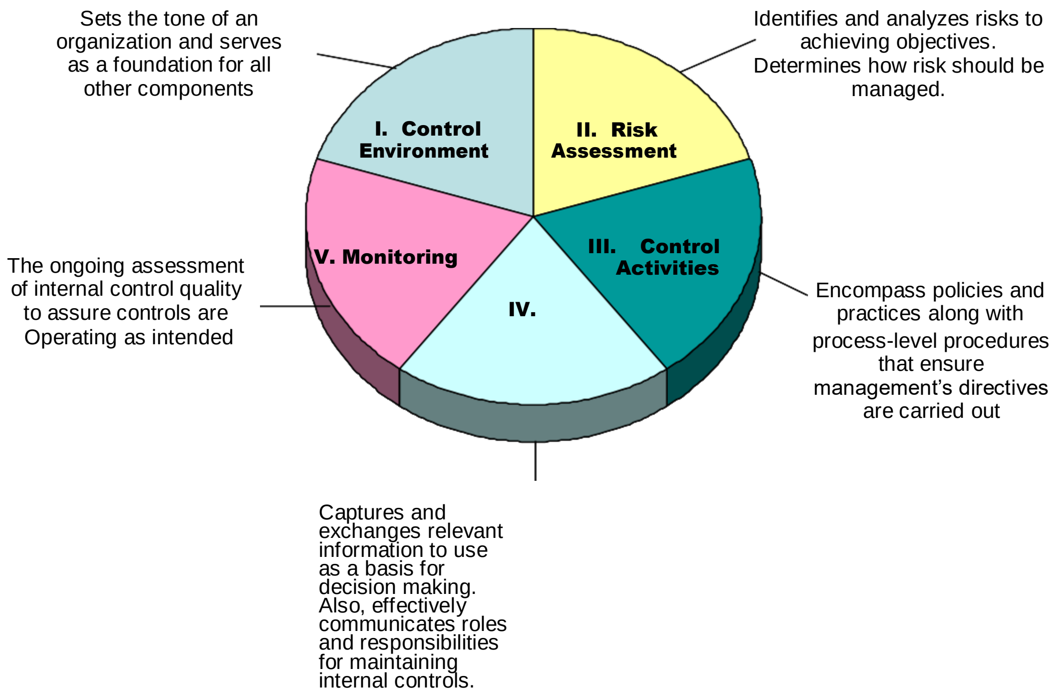
Risk reporting comprises the following elements:

- Department-specific description of key risks and opportunities.
- Description of key risk control measures including effectiveness of these control measures
- Key risk indicator for major risk categories that can be quantified like operational risks.

Risk reporting relating to the above would be generated by the Chief Risk Officer, and provided to the Risk Management Committee and Senior Management.

8. Internal Control Procedures

ERM encompasses internal control and it is an integral part of risk management and accordingly internal control system to be based on following structure:


Sets the tone of an organization and serves as a foundation for all other components
I. Control Environment
II. Risk Assessment
Identifies and analyzes risks to achieving objectives. Determines how risk should be managed.
V. Monitoring
III. Control Activities
The ongoing assessment of internal control quality to assure controls are Operating as intended
IV.
Encompass policies and practices along with process-level procedures that ensure management's directives are carried out
Captures and exchanges relevant information to use as a basis for decision making. Also, effectively communicates roles and responsibilities for maintaining internal controls.

i. **Key concepts:**

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and Board.
- Internal control is geared to the achievement of objectives in one or more separate but over lapping categories.

ii. **Key parameters:**

- Internal controls to be classified in below two categories:
  - **Preventive Controls** focus on preventing errors or exceptions. These controls can include standard policies and procedures, delegation of authority, and segregation of duties.
  - **Detective Controls** are designed to identify error or exception after it has occurred. These controls can include exception reports, reconciliations and periodic audits.

- Controls at each business to be developed based on below three primary control types:
  - **Specific Control**–Provide the frontline of defense in preventing, detecting and correcting errors.
  - **Monitoring Control**–A control, after the initial process, to detect misstatements or errors within a process.
  - **Pervasive Control**–
    A control across the organization that is not specific to a process but sets the tone of the organization.

iii. **Roles and Responsibilities as outlined by the group for Airox Technologies Limited:**

- Board is ultimately responsible for ensuring that appropriate internal control and risk management system is in place and for regularly reviewing the effectiveness of same.

- Board to delegate the responsibility to ensure the effectiveness of internal controls to Senior Management in respective business, with the objective to evaluate whether they serve to ensure:

  i. The ability to carry on the business in an orderly and efficient manner.
  ii. An adequate exchange of information between business and its investors/customers
  iii. The integrity of decision making including the treatment of all investors / customers in a fair, honest and professional manner;
  iv. The safeguarding of both its own and investor/customers assets;
  v. The maintenance of proper records and there liability of the contents of information used either within business or used for publication or distribution.
  vi. The compliance with all applicable laws and regulatory requirements.
  vii. That there is a regular and effective communication within business such that Senior Management is made aware in a timely fashion of the status of operations and financial position, including qualitative and quantitative risks posed to business, weaknesses detected, instances of non-compliance and adherence to

defined business objective; and

viii. That risk of suffering loss, financial or otherwise as a consequence of errors, frauds, defaults or changing market conditions is monitored and maintained at acceptable and appropriate levels.

ix. The existence of framework use by management as criteria for evaluating the effectiveness of internal control.

- Board is responsible for identifying the risks faced by business, assessing the risks and ensuring that there are required controls in place which are designed to ensure that any identified risk is reduced to acceptable level.

- Board to review and discuss strategic risks and opportunities arising from changes in business environment regularly and on an as needs basis.

- Risk Management Committee to be established to assist the Board in internal control and risk management.

iv. Procedures

Key risk categories for which business should have mitigation procedures in place (list not exhaustive and is indicative in nature):

- *Market Risk*
- *Credit Risk*
- *Business Risk*
- *Operational Risk*
- *Legal/Compliance Risk*
- *Fraud Risk*

v. Internal Accounting Control

The company’s system of internal accounting control should provide reasonable assurance that:

- Transactions were executed in accordance with management’s general and specific authorization.
- Transactions were recorded as necessary to permit preparation of financial statements inconformity with generally accepted accounting principles (or other applicable criteria) and to maintain accountability for assets.
- Access to assets was permitted in accordance with management’s general or specific authorization.
- The recorded accountability for assets was compared with the existing assets at reasonable intervals and appropriate action was taken with respect to any differences.

9. Glossary

Risk:	Any event that will impact achievement of the Company's objectives. Or, the level of exposure to uncertainties
Key Risks	All high risks
Risk Bank	A set of registers consisting of a list of risks, and control measures
Risk Note	Risk Note provides a snapshot of the key risks and summarizes information that can be used by management to manage risks effectively.
Risk Avoidance	A risk response strategy that entails withdrawal from activities Where additional risk and there turns are unattractive in relation to the risks faced (e.g. refuse orders, withdraw from projects);
Risk Acceptance	A risk response strategy that entails acceptance, but the potential returns are attractive in relation to the risks faced.
Risk Reduction	A risk response strategy that entails activities and measures designed to reduce the probability of risk crystallizing and/or minimize the severity of its impact should it crystallize (e.g. hedging, loss prevention, crisis management, business continuity planning, quality management).
Risk Sharing	A risk response strategy that entails activities and measures designed to transfer to a third-party responsibility for managing risk and/or liabilities for the financial consequence of risk should it crystallizes.