RISK MANAGEMENT
POLICY & FRAMEWORK

Contents

1. Introduction

1.1 Objective

The objective of this document is to establish the Risk Management policy and framework of the Company to ensure that a sound system of risk identification, risk management and related systemic and internal controls are in place to safeguard assets, resources, reputation and interests of the Company and shareholders.

1.2 Scope

All business functions, processes and sub-processes of the Company, at all locations, fall within the scope of this policy.

1.3 Exception

Exceptions are subject to the Board's approval.

1.4 Frequency of Review

This Policy will be reviewed on a yearly basis or when required, upon the occurrence of any event that requires a policy change.

1.5 Intent

The Company reserves the right to amend this policy or withdraw it in full at any time without assigning any reason.

1.6 Applicability

This Policy is applicable with effect from 23 April 2018.

2. Definitions

The following terms carry the meanings set out below wherever used in this document:

Term	Definition
Risk	The possibility of an event that could adversely affect an organization's ability to achieve its business objectives.
Risk Identification	A formal process for identifying events that could adversely affect an organization's ability to achieve its objectives.
Risk Assessment	A systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events. The risk assessment process measures risk using two factors: probability and impact.
Risk Likelihood	The measure of the relative potential/probability that the risk might occur given the operating environment and effectiveness (design and operation) of internal controls.
Risk Impact	The measure of the magnitude and nature of the effect the risk might cause given the operating environment.
Inherent Risk	The risk in the absence of a risk response.
Residual Risk	The risk after a risk response.
Risk Appetite	The amount of risk an organization is willing to accept in pursuit of value.

3. Policy & Framework

3.1 Policy

3.1.1 It is the policy of the Company to establish a risk management framework, based on the COSO Framework Model, to identify, assess, monitor and manage risks.

3.1.2 The Board of the Company is responsible for the Company's risk management strategy. Furthermore, the Board has an oversight role to determine that risk management processes are in place, adequate and effective.

3.1.3 Management of the Company is responsible for implementing the Board's strategy and for developing policies and procedures to assist the Board to identify, manage and mitigate risks across the Company's operations.

3.1.4 Risk assessment activity shall be carried out under the following circumstances at least:

(a) For review of selected business processes.

(b) For revision due to change in existing risk assessment or existing process.

(c) For induction of new business process.

(d) For new business opportunity/project risk assessment.

3.1.5 The results of the risk assessment will be used to determine the immediate actions required to mitigate high risks, including frequency of audits throughout the organization and for resource planning or efficient allocation of organizational resources.

3.1.6 Continuous monitoring and updating of the risk assessment shall be performed every year.

3.2 Framework

3.2.1 Establishing the Context of Risk Management

3.2.1.1 Management shall establish internal and external context, keeping in mind, primarily, the statutory requirements as well as customer, supplier and other stakeholders' expectations.

3.2.1.2 All risk assessments must include the identification of overall business objectives.

3.2.1.3 All risk assessments shall be done at the following three levels:

(a) Organizational Level

(b) Business Division Level

(c) Process and/or activity Level

3.2.2 Risk Identification

3.2.2.1 Risks shall be classified according to the following risk categories:

- Strategic Risk
- Operational Risk
- Reporting Risk
- Compliance Risk

3.2.2.2 Classification of risks would assist in determining the priority and assigning required control activities to relevant officials and timing of specific audit assignments in the annual audit plan.

3.2.2.3 The following sources may be considered for identification of risks:

(a) Risk Universe.

(b) Previous audit reports.

(c) Business partners' review reports.

(d) Process owner's assessment.

3.2.3 Risk Assessment

3.2.3.1 Risk assessment shall be carried out considering the significance of each risk based on two dimensions of risk:

(a) Likelihood - probability that desired objectives or outcomes will not be achieved if controls are absent or fail; and

(b) Impact - consequences of desired objective or outcome not being achieved.

3.2.3.2 Classification of Risk Likelihood

Considering the nature and frequency of risk events relevant to the process and effectiveness of internal controls in place, risk likelihood shall be categorized as follows:

Likelihood	Description
High	The risk event or circumstances of occurrence are more probable, i.e. relatively certain, or a risk event has occurred within the past year.
Moderate	The risk event or circumstances of occurrence are possible, i.e. more likely than not.
Low	The risk event or circumstances of occurrence are fairly remote.

3.2.3.3 Classification of Risk Impact

Considering the likely effect, if the risk were to materialize, on all elements of the business, i.e. Strategic, Financial, Operational, Reputational, Compliance, etc., risk impact shall be categorized as follows:

Impact	Description
High	Impact would affect business operations severely, putting business survival at risk.
Moderate	Impact would require significant time and resources to recoup.
Low	Impact would result in some possible disruptions.

3.2.4 Risk Evaluation

3.2.4.1 Taking the potential impact and likelihood into account, risk shall be evaluated or ranked as High, Moderate or Low as per the following Risk Matrix:

RISK MATRIX

		Likelihood		
		High (3)	Moderate (2)	Low (1)
Impact	High (3)	High (9)	High (6)	Moderate (3)
	Moderate (2)	High (6)	Moderate (4)	Low (2)
	Low (1)	Moderate (3)	Low (2)	Low (1)

3.2.4.2 The placement of risk on the risk matrix is the product of the weights of likelihood and impact and the risk appetite of the organization.

Risk	Weight	Explanation
High	6 or higher	The residual risk is high. Hence risk is above the acceptable tolerance level. **May Require Immediate Action.**
Moderate	Between 2 and 4	The residual risk is moderate. However, risk is within the organization's risk tolerance level. **May Require Contingency Planning.**
Low	Up to 2	The residual risk is low and within the organization's risk tolerance level. **May Not Require Immediate Action.**

3.2.5 Addressing Risk

3.2.5.1 Addressing risk shall involve identifying the options for controlling the risk, evaluating the options, developing and implementing the plan.

3.2.5.2 While addressing risk, management shall take into account the cost-benefit analysis to consider if the proposed method of treating a risk is justified.

3.2.5.3 Management shall, at its discretion and after consensus, choose to adopt any of the following risk addressing strategies:

Strategy	Description
Risk Toleration Strategy	Take no further action if there are no immediate threats or risk-mitigating controls are in place, or the risk is within tolerable level/risk appetite.
Risk Treatment Strategy	Devise/establish risk-mitigating controls within the organization.
Risk Transfer Strategy	Transfer some potential loss to another party.
Risk Termination Strategy	Terminate the activity from which the risk arises.

3.2.5.4 After treatment, the residual risk shall be managed, monitored and reviewed regularly.

3.2.5.5 Any method identified for controlling a risk shall be documented with allocated responsibility of the management team.

3.2.6 Monitoring and Review

3.2.6.1 The CEO has the responsibility to set the tone at the top of management and establish a risk management function/team within the organization.

3.2.6.2 The designated head of the risk management function will be responsible for coordinating the Company's risk management activities.

3.2.6.3 The Board may direct the internal audit function to evaluate the effectiveness and contribute to the improvement of the risk management process.