BIKAJI FOODS INTERNATIONAL LIMITED

RISK MANAGEMENT POLICY

Version	Approved by	Summary of changes	Board approval on	Date of release
Version 1	Board	Initial	13.03.2019	13.03.2019
Version 2	Board	Revised	30.12.2021	30.12.2021

❖ INTRODUCTION

Risk Management is a key aspect of the "Corporate Governance Principles and Code of Conduct" which aims to improvise the governance practices across the Company's activities. It improves decision-making, defines opportunities and mitigates material events that may impact shareholder value.

Bikaji Foods International Limited ("the Company") being a FMCG Company, is prone to inherent business risks. It desires to refine its organizational wide capabilities in risk management so as to ensure a consistent, efficient and effective assessment of risks.

The objective of the Risk Management Policy ("the Policy") is to provide the framework to manage the risks associated with its activities and to identify, evaluate, monitor and manage risks.

The 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 of Directors, Audit Committee and Risk Management Committee.

❖ LEGAL FRAMEWORK

As per section 134(3)of the Companies Act 2013, requires the Board of Directors of a Company, as part of the Board's Report, to furnish a statement a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

As per Schedule IV of the Act [Section 149(8)] - Code for Independent Directors II. Role and functions: The independent directors shall: (1) help in bringing an independent judgment to bear on the Board's deliberations especially on issues of strategy, performance, risk management, resources, key appointments and standards of conduct; (4) satisfy themselves on the integrity of financial information and that financial controls and the systems of risk management are robust and defensible.

As per section 177(4)(vii) of the Companies Act 2013, every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include, evaluation of internal financial controls and **risk management systems**.

Regulation 17(9) of the Listing Regulations requires the Company to lay down procedures about risk assessment and risk minimization.

As per Regulation 21 and Para C of Part D of Schedule II of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulation, 2015"), every listed entity shall constitute a Risk Management Committee and such committee shall formulate a detailed risk management policy which shall include:

(a) A framework for identification of internal and external risksin particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee;
(b) Measures for risk mitigation including systems and processes for internal control of identified risks;
(c) Business continuity plan.

The Board of Directors, Audit Committee and Risk Management Committee is responsible to ensure that the Company has a robust Risk management framework and monitor its effectiveness on periodic basis.

❖ APPLICABILITY

This policy applies to all functions of the Company and its subsidiaries.

❖ OBJECTIVE & PURPOSE OF POLICY

The Company operates in an environment that is highly Volatile, Uncertain, Complex and filled with Ambiguity, where effective risk management is a key for business growth.

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, in order to guide decisions on risk related issues.

Objectives of the Policy:-

1. To ensure that all the current and future material risk exposures of the Company are identified, assessed, quantified, appropriately mitigated, minimized and managed i.e., to ensure adequate systems for risk management.

2. Providing a framework that enables future activities to take place in a consistent and controlled manner.

3. Evaluating the likelihood and impact of major adverse events.

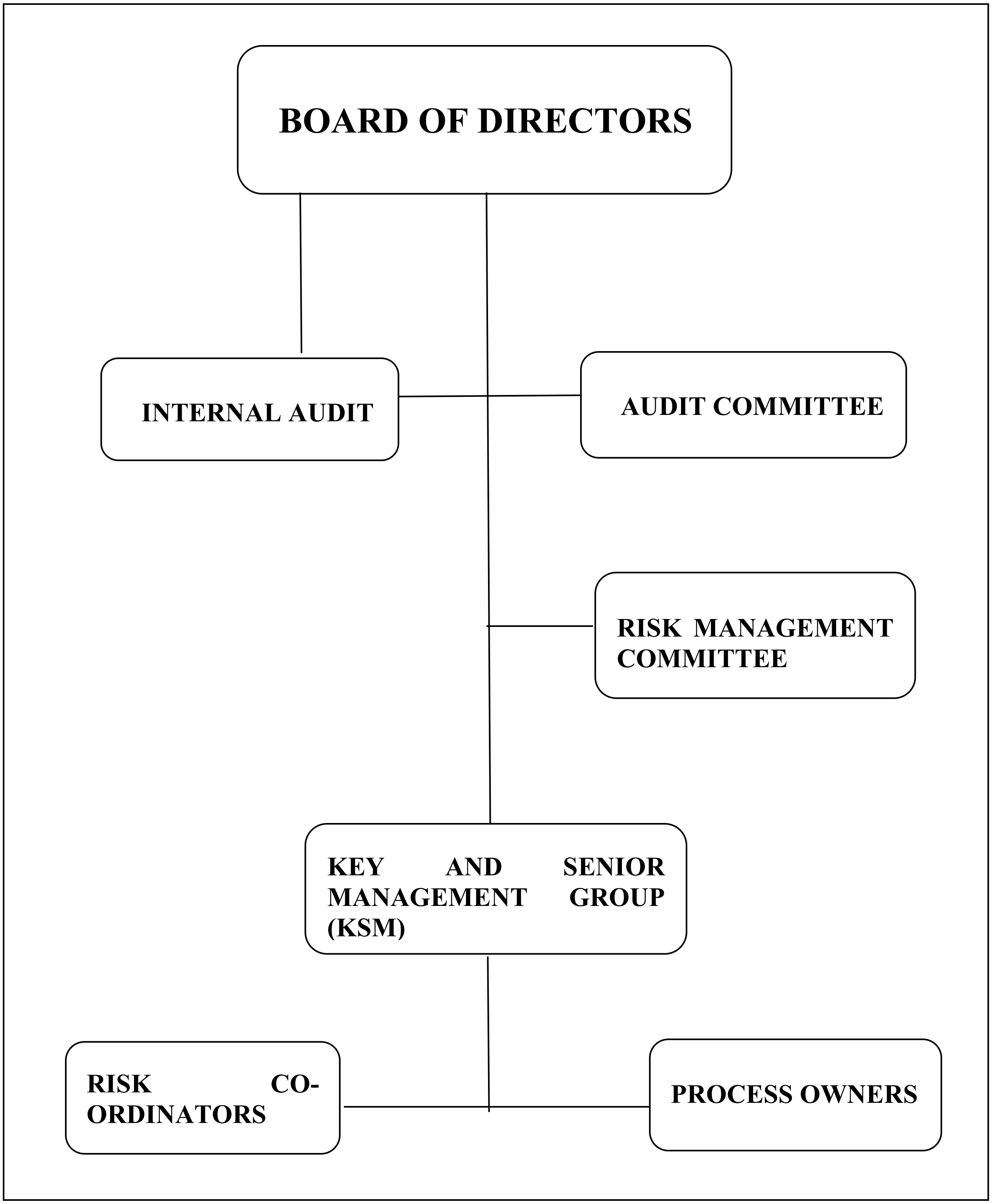
4. To ensure compliance with appropriate regulations, wherever applicable, through the adoption of best practices.

5. To assure business growth with financial stability.

6. To formulate Business Continuity Plan.

❖ RISK ORGANISATION STRUCTURE

The risk organization structure of the Company as follows:



❖ ROLES AND RESPONSIBILITIES

Board of Directors:-

1. Approve and review the Risk Management Policy.

2. Identify and assess internal and external risks in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk that may impact the Company in achieving its strategic objectives or may threaten the existence of the Company.

3. The Independent Directors shall help in bringing an independent judgment to bear on the Board's deliberations on issues of risk management and satisfy themselves that the systems of risk management are robust and defensible.

4. Give directions to the Audit Committee and Risk Management Committee on top priority risks identified and its mitigation plan.

5. Be satisfied that processes and controls are in place for managing less significant risks.

6. Ensure risk management is integrated into board reporting and annual reporting mechanisms.

7. Board shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit (such function shall specifically cover cyber security).

Audit Committee:-

1. Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include, evaluation of internal financial controls and risk management systems.

Risk Management Committee:-

1. To formulate a detailed risk management policy which shall include:

   (a) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
   (b) Measures for risk mitigation including systems and processes for internal control of identified risks
   (c) Business continuity plan.

2. To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.

3. To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.

4. To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.

5. To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken:

   (a) To update Risk Register on half-yearly basis.
   (b) To report key changes in critical risks to the Board.
   (c) To report all critical risks to the Board in detail on yearly basis.

6. The appointment, removal and terms of remuneration of the Chief Risk Officer (i.e. Chief Financial Officer {"the CFO"}) shall be subject to review by the Risk Management Committee.

7. The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.

8. The Committee shall meet at least twice in a year in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

9. To perform such other functions as may be prescribed by the Board of Directors from time to time.

Key and Senior Management Group (KSM) including Chief Risk Officer:-

1. Implement and monitor the principles, actions and requirements of the risk management plan.

2. Review risks on quarterly basis- identification of new risks, changes to existing risks, updating risk register etc.

3. Internal compliance and control systems (inclusive of cyber security cover) for the implementation of the risk management plan and to ensure that the system is operating effectively in relation to financial reporting risks.

4. Reporting to the Board of Directors, Audit Committee and Risk Management Committee on risks and mitigation strategies on regular intervals.

5. To assist the Board in discharging its responsibility in relation to risk management.

Risk Co-ordinators and Process Owners:-

1. Ensure the implementation of recommendation and action plan finalized by the Board and facilitating execution of Risk Management practices in the organization.

2. Identify any perceived risk at ground level in various processes.

3. Working closely with business units, business enabling functions and mitigation action owners in deploying mitigation measures and monitoring their effectiveness

4. Ongoing maintenance of risk framework and documentation including policies and procedures.

5. Providing periodic updates to the Chief Risk Officers and quarterly updates to the Key and Senior Management Group on risks to key business objectives and their mitigation.

6. Suggesting best practices for strengthening the risk management process.

❖ RISK MANAGEMENT SYSTEM

The Company has always had a system-based approach to business risk management. Backed by strong internal control systems, the current risk management framework consists of the following elements:
-Risk Management system is aimed at ensuring formulation of appropriate risk management– policies and procedures, their effective implementation and independent monitoring and reporting by Internal Audit.

-A combination of centrally issued policies and divisionally-evolved procedures brings robustness– to the process of ensuring business risks are effectively addressed.

-Appropriate structures have been put in place to effectively address inherent risks in businesses– with unique / relatively high-risk profiles.

-A strong and independent Internal Audit Function at the corporate level carries out risk focused– audits across all businesses, enabling identification of areas where risk managements processes may need to be improved. The Board reviews internal Audit findings, and provides strategic guidance on internal controls. Monitors the internal control environment within the Company and ensures that Internal Audit recommendations are effectively implemented.

The combination of policies and processes as outlined above adequately addresses the various risks associated with our Company's businesses. The Senior Management of the Company periodically reviews the risk management framework to maintain its contemporariness so as to effectively address the emerging challenges in a dynamic business environment.

❖ RISK IDENTIFICATION

Each unit, business division and functional department is responsible for identifying the probable risks in their areas of operation, which is then escalated to the management level. The Risk Co-Ordinator coordinates with all departments, seeking updation of existing risks include Financial, Operational, Reputational, Regulatory, Third-party, Sustainability, Social, Environmental and Technological Risks as well as identification of new, emerging risks in their respective areas.

I. Risk Register:-

Risk register shall be maintained and be periodically signed by the Chief Risk Officer. Periodicity should be minimum once in a year or whenever there is change in Risks, whichever is earlier

II. Risk Register Updation:-

Risk Register is updated on half-yearly basis in the following manner: -

(a) Internal Audit Department co-ordinates with all the Units, Divisions and Departments seeking updation in existing risk as well as for new risk emerged in their respective areas if any.

(b) New risk received from Units and Divisions if any are confirmed by concerned process owners at Corporate Office.

(c) All updates received from respective process owners including Mitigation plan are updated in draft Risk Register by Internal Audit Department and discussed internally in presence of Chief Risk Officers for their inputs before presentation to KSM.

(d) Inputs based on internal discussion are incorporated in the draft Risk Register before presentation to KSM and post presentation to KSM, inputs suggested by KSM are also updated in the draft Risk Register.

(e) Post incorporation, these changes are again discussed internally with Chief Risk Officers for their review and then presentation is circulated to the Risk Management Committee as part of committee agenda papers. Post confirmation by Risk Management Committee, the risks are updated in the Risk Register.

❖ RISK REPORTING

Risk Management Presentation is made to KSM and Risk Management Committee at half-yearly frequency.

(a) An annual updated Risk Management Presentation shall be made to the Board once in a year.

(b) Key Changes in the Risks (i.e. addition of new Risk or removal of a mitigated risk), identifying any new risk, modifying existing risk, scanning external environment for emerging risk and accordingly updating the priority for risks shall be updated to Board on half–yearly basis.

(c) Risk Management Systems shall be presented to the Audit Committee once in a year for their evaluation.

(d) The Risk Management Committee meets at least twice in a year in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

❖ BUSINESS CONTINUITY PLAN

Business Continuity Plans are required to be defined for risks corresponding to High Impact and High Velocity to enable rapid response to address the consequence of such risks when they materialize.

A detailed business continuity plan shall be undertaken periodically with an objective to ensure in case of any eventuality of High-Risk Nature, they are addressed immediately within 24 hours with no disruption in the business including Production and Sales and related financial transaction processing. KSM shall be the Crisis Management Team who shall be responsible for laying out crisis response mechanism, communication protocols, and periodic training and competency building on crisis management and can invite internal or external persons to plan and implement mitigation action plan.

Mitigation Plan:-

In case of occurrence of an event leading to particular plant shutdown, alternative arrangements should be made at another plant or at third party manufacturing location immediately without any loss of Production/Sales.

In case of critical IT application disaster or cyberattack, mitigation action should be implemented immediately within the defined time limits to restore the impacted application or an alternative application or the same application from an alternative place.

The Business Continuity Plan should be tested for its effectiveness at periodical intervals not exceeding three years to ensure company is well prepared to manage any crisis event and ensure Business Continuity.

❖ DISCLOSURE IN BOARD'S REPORT

The Board of Directors shall include a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

❖ POLICY REVIEW

The Committee shall be reviewing the Risk Management Policy at least once in two years, including by considering the changing industry dynamics and evolving complexity to ensure effectiveness and that its continued application and relevance to the business.

Feedback on the implementation and the effectiveness of the policy will be obtained from the risk reporting process, internal audits and other available information.

❖ AMENDMENTS

In case of any subsequent changes in the provisions of the Companies Act, 2013, the Listing Regulations, 2015 or other applicable law, which makes any of the provision in the Policy inconsistent with the Act or Listing Regulations, 2015 or law, then the provisions of the Companies Act, 2013, Listing Regulations, 2015 or law would prevail over the Policy and the provisions of the Policy would be modified in due course to make it consistent with law.