Enterprise Risk Management Policy

Prataap Snacks Limited

CONTENT

1. Background

Section 134 of the Companies Act, 2013 **("the Act")** requires a statement to be included in the report of the Board of Directors of the company 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.

Further, as per Regulation 17 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, **("the Listing Regulations")**, the listed entity shall lay down procedures to inform members of Board of Directors about risk assessment and minimisation procedures. The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity. As per Regulation 21 of the Listing Regulations, the Board of Directors 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.

The Company recognises that Effective Risk Management Is Integral To Its Long-Term Success, safeguarding stakeholder value and supporting strategic objectives. The policy seeks to embed a structured and proactive risk culture consistent with best practices adopted by leading FMCG companies.

2. Objective

The purpose of the Enterprise Risk Management (ERM) Policy is to institutionalise a formal risk management function and framework in the Company for identifying, assessing, monitoring and managing its business risk, including any material changes to its risk profile. This ERM Policy has been prepared in accordance with the guidelines provided under the Act and Listing Regulations.

Prataap Snacks Limited has adopted ERM Policy in order to effectively manage the risks associate with its business and in working towards its business objectives and goals.

The Policy also aims to:

1. Promote Awareness and Accountability for Risk at All Levels of Management.
2. Integrate Risk Considerations into Strategic Planning, Capital allocation and Decision-Making.
3. Ensure Alignment with the Company's ESG (Environmental, Social, Governance) Objectives and Sustainability Roadmap.
4. Strengthen Cybersecurity Readiness and Data Privacy Controls.

3. Definitions

- **Board**: The Board of Directors of the Company.
- **ERM**: Enterprise Risk Management.
- **RMC**: The Risk Management Committee of the Board.
- **CRO**: The Chief Risk Officer of the Company.
- **Functional Heads**: The heads of the various departments or functions within the Company such as Finance, Operations, Supply Chain, Sales & Marketing, Human Resources, Information Technology (IT), Legal & Compliance, and any other key function as may be designated from time to time.
- **Risk Owner**: The individual (typically a Functional Head or delegated delegate) responsible for managing a particular risk, its mitigation plans and monitoring.
- **Key Risk Indicator (KRI)**: A metric used to signal an increase in risk exposure, providing early warning.
- **Heat-map**: A visual tool representing each risk on axes such as likelihood and impact, typically colour-coded (High/Medium/Low).

4. Risk Management Framework

Prataap Snacks Limited has adopted this Policy to effectively manage risks associated with its business and in working towards its business objectives through the following structured steps:

- Risk Identification
- Risk Assessment/ Quantification
- Risk mitigation & control implementation

Continuous Monitoring, reporting and review of Risk Additionally, the Company will:

- Maintain a Formal Risk Register which is Updated Quarterly and reviewed by the Risk Management Committee.
- Classify Risks as Strategic, Operational, Financial, Compliance, ESG, and Cybersecurity.
- Call out the risk owner and identify mitigation plans in the short and long term.
- Ensure that Risk Mitigation Actions are Linked to Performance Indicators and Internal Control Systems
- Call out a senior executive as the CRO

5. Scope

This Policy applies to all functions, locations, and operations of the Company, including its subsidiaries, contract manufacturing units, joint ventures, and key partners where applicable.

It covers all major categories of risk including — strategic, operational, supply chain, financial, regulatory, environmental & social (ESG), cyber security, and reputational risks.

6. Risk Appetite

A critical element of the Company's risk-management framework is the risk appetite, which is defined as the extent of willingness to take risks in pursuit of the Company's business objectives. The key determinants of the Company's risk appetite include:

- Shareholder and investor preferences and expectations;
- Expected business performance (return on capital);
- The capital needed to support risk-taking;
- The culture of the organisation;
- Management experience along with risk and control-management skills; and
- Longer-term strategic priorities.

Appetite Levels by Risk Domain

Risk Domain	Appetite Level	Rationale & Boundaries
Strategic Growth / Innovation	High	The Company is willing to take higher risk for new growth initiatives (new geographies, product launches, brands or strategic alliances) provided robust mitigation, business case and controls are in place.
Market & Commodity Volatility	Medium	The Company accepts moderate variability in commodity costs, exchange rates or competitive pressures, given the FMCG environment, but expects hedging, responsiveness and margin management.
Financial & Capital Risks	Medium	While growth is important, the Company aims to maintain prudent leverage, liquidity and return metrics. Losses beyond thresholds or deterioration of solvency are not acceptable
Operational / Supply-chain Risks	Low to Medium	The Company seeks to ensure continuity of operations, quality, manufacturing and distribution. Disruptions must be kept within controllable limits. Appetite is lower for those risks that may impact meeting customer demand or cost structure materially.

Compliance / Legal / Regulatory	Low	The Company has very little appetite for risks that could lead to regulatory breaches, fines, legal exposures or loss of license.
Reputation / Brand / Product-Safety	Very Low	The Company places brand trust and consumer confidence as critical assets; risk exposures that can seriously damage brand or stakeholder trust are unacceptable. The appetite is effectively zero for events that could cause major brand erosion or consumer harm.
Cybersecurity / Data-Privacy	Low	With increasing digitalisation, the Company has low appetite for cyber / data-breach incidents that could disrupt operations or leak customer data. Investments in controls, monitoring and response must keep residual risk within tolerance.
ESG / Environmental / Social	Low	Given the Company's commitment to sustainability, the appetite for risks that impair environmental compliance (e.g., water/pollution risk), labour standards, social license to operate or governance is very low. The Company will not accept major exposures in these areas.

The Company communicates its risk appetite through its strategic plans. The Board and senior management monitor the Company's exposure relative to its stated risk appetite and actual results to ensure an appropriate level of risk tolerance throughout the organization.

6.1 Quantitative and Qualitative Boundaries

- The Company will define, for each major risk category, tolerance thresholds (e.g., maximum % EBITDA loss, maximum working-capital days, maximum number of incidents) that must not be exceeded. This aligns with the "green/amber/red" risk-exposure zones seen in frameworks.
- The Company will adopt a "traffic-light" heat-map approach (Green = within appetite; Amber = approaching limit; Red = breach) and will require immediate escalation if exposure moves into Amber/Red.
- For strategic initiatives, risk appetite will be considered as part of business-case approval: projects that lead to exposures beyond defined thresholds or outside of tolerance must be justified to the RMC/Board and may be rejected or require additional mitigation.
- Qualitative guidance: Risk appetite statements will be embedded into decision-making,
- Monitoring via Key Risk Indicators (KRIs): each risk domain will have KRIs aligned to appetite thresholds (e.g., number of data-breaches, supply-chain downtime hours, package violation events, regulatory notices). Exceeding KRI triggers leads to action.

6.2 Governance, Review & Escalation

- The Board sets the overarching risk appetite and receives quarterly reports from the Risk Management Committee (RMC) on actual risk-exposures versus appetite.
- The RMC monitors at least bi-annually (or more frequently, as required) the risk profile, noted deviations, emerging risks and need to recalibrate appetite.
- The CRO (Chief Risk Officer) ensures risk-appetite is cascaded into functional planning, monitored via dashboards, and any breaches or near breaches are escalated outside the cycle.
- Functional Heads and Risk-Owners are accountable for operating within defined appetite boundaries and must escalate if residual risk is trending to exceed tolerance.
- The Company will review risk appetite at least annually (or upon significant change in business model, regulatory environment, supply-chain structure or strategic direction) to ensure alignment with business, external environment and stakeholder expectations.

7. Risk Governance Structure & Roles & Responsibilities
7.1. Board of Directors

The Board of the Company shall:

- Oversee and approve the Company's ERM Policy and framework.
- Define and approve the Company's risk-appetite and ensure that management acts within those parameters.
- Review at regular intervals a report from the RMC on the risk profile, material risks, mitigation status and changes in risk-exposure.
- Ensure that the risk-management systems are adequate and functioning.
- Evaluate the effectiveness of risk management, and challenge strategic assumptions and exposures.

7.2. Risk Management Committee (RMC)

- Constituted by the Board, the RMC shall assist the Board in risk oversight.
- The RMC shall comprise at least three members of the Board (including at least one Independent Director) plus senior executive(s) as decided by the Board.
- The RMC will meet at least twice a year (and not have a gap of more than 180 days between meetings) or more frequently if needed.
- Responsibilities include: reviewing and evaluating risk-management systems; approving the risk-register; reviewing the heat-map, dashboard and KRIs; ensuring business continuity plans; monitoring cyber-security exposures; escalating major emerging risks to the Board.

7.3. Chief Risk Officer (CRO)

- The Company shall appoint a senior executive as the CRO. The CRO shall not have direct commercial or business-vertical targets or responsibilities that create conflicts with objective risk oversight.
- The CRO shall report functionally to the RMC to preserve independence and shall have access to the Board/RMC.
- Key responsibilities of the CRO include: maintaining the enterprise risk-register; coordinating risk-identification and assessment across functions; facilitating mitigation plan formulation; tracking implementation, KRIs, dashboards; educating the organisation on risk culture; presenting risk updates to the RMC; supporting the Board/RMC in recalibrating risk appetite and framework. This independent role is important and aligned with best practice.

7.4. Chief Executive Officer (CEO)

- The CEO is responsible for overseeing implementation of the ERM Policy, analysing risks identified by functional heads in consultation with the CRO, developing strategies/measures to contain identified risks, and ensuring periodic monitoring.
- The CEO shall direct the CRO and convene the RMC and ensure risk culture is embedded in strategic planning, decision-making and operations.

7.5 Functional Heads & Risk Owners

- Each Functional Head (Finance, Operations, Supply Chain, Sales & Marketing, HR, IT, Legal & Compliance, etc) is responsible for identifying business risks in their area (internal and external) and ensuring implementation of mitigation strategies.
- The functional heads shall nominate risk owners within their respective functions. Risk Owners shall manage the risk-mitigation plans, monitor KRIs and report regularly to the CRO and RMC.
- Risk ownership shall be clearly defined; the risk owner is best placed to coordinate mitigation actions.

8. Risk Management Framework

8.1 Risk Identification

- Functional Heads shall identify business-risks (internal and external) across categories such as strategic, operational, key raw material pricing, financial, sectoral, legal, sustainability (including ESG), cyber-security or any other risk.

- The risk-identification exercise shall be done at least annually, and more frequently if requested by the CEO or CRO.
- Risks must be identified with reference to each strategic business objective.
- Additionally, risk identification shall include benchmarking with peer companies, review of regulatory developments and scanning of external environment (industry, competitors, technology, macro) that may impact operations, brand-reputation or compliance.
- Emerging risks shall be notified immediately by functional heads to the CEO/CRO for further evaluation.

8.2 Risk Assessment & Prioritization

- Each identified risk is assessed in terms of:

  a. probability of occurrence,
  b. impact (on objectives, revenues, reputation, operations),
  c. velocity (how quickly risk impact may occur) and
  d. criticality.

The Company may adopt a scoring scale (e.g., 1-3 for likelihood, 1-3 for impact) to arrive at a "criticalness".

- The Company will deploy a heat-map (risk matrix) for visual representation of key risks—each risk will be rated High/Medium/Low and regularly reviewed.
- Risks that exceed defined thresholds (in line with risk appetite) will be flagged for stronger controls and escalations.

8.3 Risk Response (Mitigation, Transfer, Acceptance)

- For each high-critical risk, a documented mitigation plan shall be developed: identifying risk owner, short-term and long-term actions, link to KRIs and performance metrics, internal control systems, responsibilities, timelines and resources.
- Risk responses may include: avoidance (stop the activity), mitigation (reduce likelihood/impact), transfer (insurance, contracts), acceptance (within appetite) or exploitation (where opportunity risk).
- Mitigation actions will be linked to functional KPIs and performance management systems.
- The Company shall ensure that risk mitigation strategies integrate with operational decision-making, capital allocation and sustainability/ESG objectives.

8.4 Risk Monitoring, Reporting & Key Risk Indicators (KRIs)

- A Formal Risk Dashboard shall be placed before the RMC every quarter.
- KRIs shall be defined for each significant / high risk to enable early-warning signals and trigger corrective action.
- Risk owners shall monitor KRIs, review mitigation progress, report deviations and emerging risks.
- The CRO shall consolidate dashboards, heat-maps, risk register updates and present to the RMC.
- Bi-annual enterprise risk-review meetings shall be conducted involving the functional heads, CEO, CFO and CRO.
- Emerging risks or surprises shall be escalated outside the regular schedule if they breach risk-appetite or tolerance.

8.5 Business Continuity Planning & Resilience

- The Company shall ensure that a plan/procedure is in place that outlines how its business will continue operating during an unplanned disruption (pandemic, supply-chain breakdown, cyber-attack, natural disaster).
- The business continuity plan shall contain contingencies for business processes, assets, financial resources, human resources, business partners and any aspect that might be affected, with possible solutions.

- The plan shall be tested periodically (at least annually) and updated in light of learnings.

9. Risk Register, Dashboard & Heat-map

- The Company shall maintain a formal risk register which is updated quarterly, reviewed and approved by the RMC.
- The register shall classify risks under categories (Strategic, Operational, Financial, Compliance, ESG, Cybersecurity) and identify risk-owner, mitigation plans, KRIs, status of controls and due dates.
- A risk heat-map (likelihood vs impact) shall depict current risk exposures visually.
- The risk dashboard will provide summary for Board/RMC: top risks, their status, emerging risks, changes in profile, KRIs trending, mitigation progress.
- The register and dashboard shall link to performance indicators, internal controls and decision frameworks.

10. Review of risk management

The Company regularly evaluates the effectiveness of its risk management program to ensure that its internal control systems and processes are monitored and updated on an ongoing basis.

11. Amendment

This ERM Policy shall be reviewed by the R M Committee/Board as and when any changes are to be incorporated in the Policy due to changing industry dynamics and evolving complexity or change in law or as may be felt appropriate by the R M Committee/Board. Any changes/amendment/modification in the Policy will be in writing and approved by Board of Directors of the Company on recommendation of the R M Committee.

The latest approved version shall be circulated to all Functional Heads and hosted on the Company's Website, in line with good governance practice.

Reviewed on: November 4, 2025
Approved on: November 4, 2025

Mr. Arvind Kumar Mehta
Chairman and Executive Director
Board of Directors
DIN: 00215183