Lenskart Solutions Limited

(Formerly known as Lenskart Solutions Private Limited)

Risk Management Policy

August 2026

Table of Contents

1. Introduction 3
   1.1. Context 4
   1.2. Objective 4
   1.3. Scope 4
   1.4. Revision 4
2. Risk governance 5
   2.1. Risk Management Structure 6
   2.2. Risk Management Roles and Responsibilities 6
      2.2.1. Board of Directors (BOD) 6
      2.2.2. Risk Management Committee (RMC) 6
      2.2.3. Risk Officer 7
      2.2.4. Risk Owner(s) 7
      2.2.5. Mitigation action owner(s) 7
3. Risk Management Framework 8
   3.1. Enterprise risk management framework 9
      3.1.1. Step 1: Identify Risks 9
      3.1.2. Step 2: Prioritize Risks 10
      3.1.3. Step 3: Risk Response Strategies 11
      3.1.4. Step 4: Monitor Risks 12
      3.1.5. Step 5: Reporting 12
   3.2. Risk Workshop 12
4. Annexure 14
   4.1. Risk Register & Mitigation Template 15

1. Introduction

1.1. Context

Lenskart Solutions Limited ("Lenskart" or the "Company") operates in a dynamic business environment characterized by rapid technological advancements, integrated manufacturing, and a growing global omnichannel footprint across India, Southeast Asia, Japan, and the Middle East.

As the Company transitions to a listed entity, it is imperative to establish a robust Risk Management Policy in accordance with the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations") and the Companies Act, 2013. This policy is designed to align with the Listing Agreement and best-in-class international standards (such as ISO 31000), ensuring that the Company can proactively navigate uncertainties while protecting shareholder value.

1.2. Objective

The primary objective of this Policy is to institutionalize a structured mechanism for handling uncertainty. Specifically, the framework aims to:

- **Enhance Board Visibility**: Provide the Board of Directors with a transparent, consolidated view of the top risks threatening the Group's strategic goals.
- **Strengthen Risk Governance**: Establish clear ownership and accountability for risk management at all levels—from the Board down to operational function heads.
- **Standardize Identification & Evaluation**: Ensure a uniform methodology is used across the Group to identify, assess, and prioritize risks based on business impact and likelihood.
- **Drive Effective Mitigation**: Move beyond identification to action by ensuring every material risk has a concrete mitigation plan and an assigned owner.
- **Embed Reporting & Improvement**: Facilitate regular reporting to the Risk Management Committee to monitor the effectiveness of controls and drive continuous improvement in the risk framework.

1.3. Scope

This Policy applies to Lenskart Solutions Limited and all its subsidiaries, joint ventures, and associates globally (collectively, the "**Group**"). It encompasses all functions, geographies, and levels of the organization.

The scope covers all Events—internal or external—that could adversely impact the Group's strategy, operations, financial position, or reputation. This includes, but is not limited to, strategic, operational, financial, compliance, cyber security, and ESG (Environmental, Social, and Governance) risks.

1.4. Revision

This policy shall be reviewed periodically or at the frequency defined by the applicable regulations to assess the need for any revision or update.

Revision history

This document has been reviewed and approved by:

Version	Author	Date	Revision	Reason or Change in Description	Reviewer and Approver
2.0	-	12.08.2026	1st revision	Approval of revised policy by Board.	Legal, IA and Board

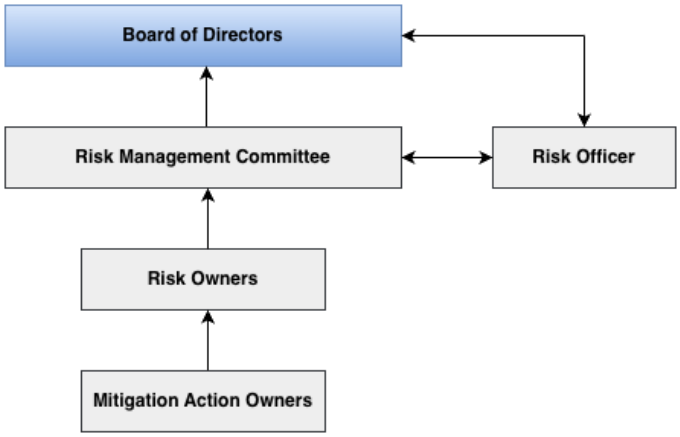
2. Risk governance

2.1. Risk Management Structure

The risk governance structure at Lenskart is designed to ensure independence, accountability, and active oversight.

- The **Board of Directors** holds the ultimate responsibility for the Company's risk management framework.
- To discharge this duty effectively, the Board has constituted a **Risk Management Committee (RMC)**, a sub-committee of the Board, specifically tasked with overseeing the implementation and monitoring of the risk policy.
- The RMC shall designate a **Risk Officer** who will be responsible for the day-to-day orchestration of the risk framework.

The Risk Management Structure adopted by the company is illustrated below:



2.2. Risk Management Roles and Responsibilities

2.2.1. Board of Directors (BOD)

- **Ultimate Responsibility**: Retains overall responsibility for the development and implementation of the Risk Management Policy and Plan.
- **Risk Appetite**: Defines and approves the Company's "Risk Appetite", the level of risk the Company is willing to accept in pursuit of its strategic objectives.
- **Annual Review**: Reviews the effectiveness of the risk management framework and processes at least once annually to ensure they remain fit for purpose.

2.2.2. Risk Management Committee (RMC)

- **Oversight & Monitoring**: Oversees the implementation of the risk management policy, monitors the robustness of the risk management framework, and evaluates the adequacy of risk management systems.
- **Risk Review**: Periodically reviews the Risk Register to ensure that material risks, including Cyber Security and ESG risks, are being identified, evaluated, and mitigated effectively.
- **Mitigation Guidance**: Reviews the mitigation steps proposed by the management and recommends further action where necessary to bring risks within acceptable limits.
- **Policy Formulation**: Formulates and recommends modifications to the Risk Management Policy to the Board for approval.

2.2.3. Risk Officer

- **Custodian:** Acts as the primary custodian of the Risk Management Policy, ensuring it is communicated and understood across the organization.
- **Coordination:** Facilitates the risk identification and assessment workshops with business functions and consolidates the Group Risk Register.
- **Advisory:** Acts as an internal advisor to business heads on risk-related matters.

2.2.4. Risk Owner(s)

- **Identification:** Responsible for the timely identification of risks within their specific business unit or function.
- **Assessment:** Evaluates the likelihood and impact of risks using the Company's standard criteria.
- **Mitigation:** Designs and implements adequate internal controls and action plans to mitigate identified risks.

2.2.5. Mitigation action owner(s)

- **Implementation:** Executes specific mitigation strategies and internal controls within the function as assigned by the Risk Owner.

3. Risk Management Framework

3.1. Enterprise risk management framework

The Company adopts a continuous, cyclical risk management process designed to provide early visibility into potential threats and opportunities. This framework ensures that risk management is not a periodic compliance exercise but an integral part of strategic decision-making.

The overall design of the framework follows a five-step lifecycle:

3.1.1. Step 1: Identify Risks

Identification is the process of recognizing and recording uncertainties that could impact the achievement of strategic or operational objectives. We do not rely on a single source; instead, we aggregate insights from:

- Strategic Reviews: Analysis of market trends, competitor moves, and regulatory changes.
- Operational Feedback: Inputs from functional heads, and internal audit findings.
- External Events: Geopolitical shifts, cyber threat intelligence, and macroeconomic factors.

This process is conducted via structured workshops, interviews, and historical data analysis to ensure a comprehensive risk universe is captured.

Company shall classify all applicable enterprise risks for the Company in below stated broad categories:

Risk Classification	Risk drivers
Sectoral	Key sectoral risks applicable to all entities in the Retail sector
Operational	Inadequate or failed processes or people capabilities
Financial	Related to Financing / financial transactions
Information & Cyber	Possible information / data leakage, misuse, or loss / Cyber Threats/frauds
Strategic	Related to strategic initiatives

Compliance & Regulatory	Related to financial regulations, labour laws, import/export etc
Sustainability (ESG)	Related to environment, social and governance
People/HR	Related to Employee Development/ Talent Management/ Succession Planning

Since risk identification is a continuous process, management is encouraged to identify and report significant risks that may exist or are likely to occur. Mitigation action owners and risk owners to identify and update risk register biannually.

The risk identification formats shall together constitute the 'Risk Register' for each department. Refer Annexure 4.1 for the risk register template.

3.1.2. Step 2: Prioritize Risks

Not all risks warrant equal attention. We assess identified risks based on three dimensions to determine their Materiality:

- Likelihood: The probability of the risk event occurring (Rare to Almost Certain) assuming no controls in place or suddenly fail.
- Impact: The potential severity of the consequence on financials, reputation, legal compliance, or operations (Insignificant to Critical) assuming no controls in place or suddenly fail.
- Control Effectiveness: The perceived effectiveness of the existing controls that will reduce the inherent risk level.

The overall risk score is expressed as the Risk Assessment Number (RAN), computed as: RAN = Impact × Likelihood × (6 − Control Effectiveness). A higher RAN denotes a higher level of residual risk requiring priority attention.

The parameters for impact, and likelihood laid down by the company for the purpose of risk assessment are as follows:

Impact

Potential consequence if the risk occurs — yearly EBITDA/Cash impact, assuming no controls are in place or suddenly fail.

Score	Level	Yearly EBITDA impact
5	Critical	>20%
4	Major	>10% - 20%
3	Moderate	>5% - 10%
2	Minor	>1% - 5%
1	Insignificant	0% - 1%

Likelihood

Chance of the risk occurring over the plan period — % probability, assuming no controls are in place or suddenly fail.

Score	Level	% Probability
5	Almost Certain	>80% (surprise if not happens)
4	Likely	>50% - <80% (more likely to happen than not)
3	Possible	>10% - <50% (likely to happen)
2	Unlikely	>1% - <10% (Less Likely to happen)
1	Rare	>0% - <1% (surprise if happens)

Control Effectiveness

Perceived effectiveness of existing controls — % reduction of the inherent risk level. Higher score is better.

Score	Level	% Risk reduction
5	Very high	>80%
4	High	>50% - <80%
3	Medium	>20% - <50%
2	Low	>5% - <20%
1	Very low	>0% - <5%

** Controls include any process, policy, device or practice specifically taken to modify the impact or likelihood of a risk.*

Risk Assessment Number (RAN) = Impact × Likelihood × (6 – Control Effectiveness)

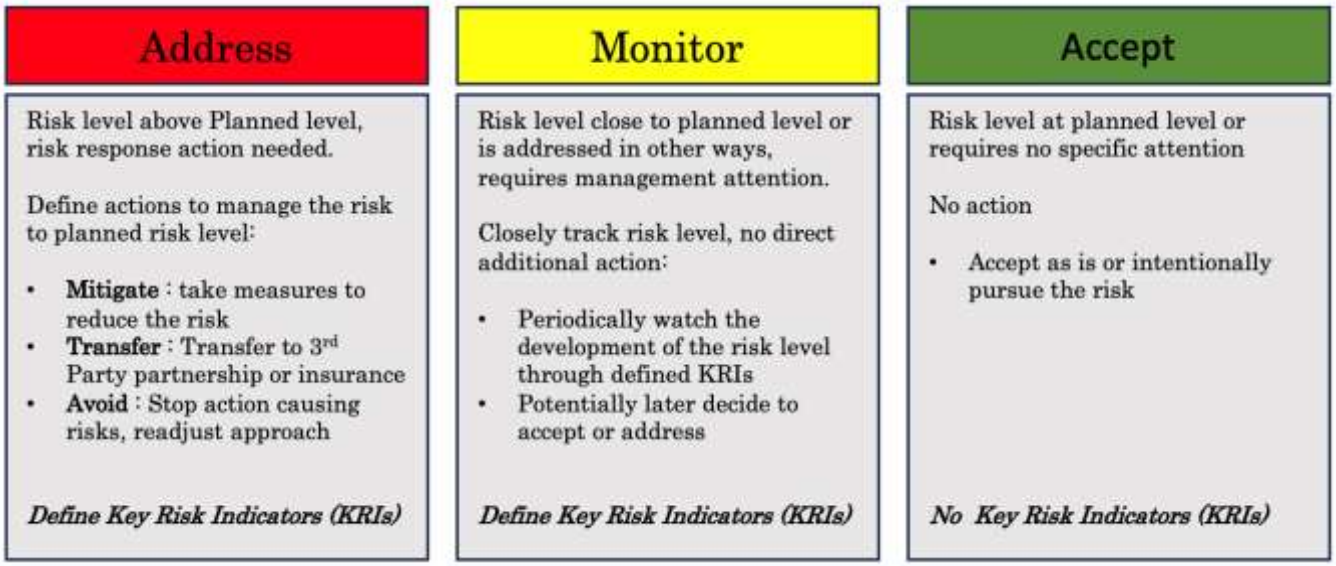
3.1.3. Step 3: Risk Response Strategies

Evaluation must translate into action. For every material risk, a Risk Owner must define a clear treatment strategy.

First line Management evaluates if what we do today provides the comfort we need, or if further action is needed to manage the risk to planned level. The risks response is different for each of the below strategies:

- Address is the response resulting in defined actions to bring the risk to planned level.
- Monitor means no action but at least quarterly watch how the risk evolves.
- Accept means no action nor active tracking.

Management can adjust the response strategy as needed over time. When response actions result in a lower level the strategy can be adjusted from Address to Monitor.



Key Risk Indicators

As the risk exposure of any business may change due to continuously changing environment, the risks with their mitigation measures shall be updated regularly. This can be updated based on early warning indicators.

Key risk indicators are rule based quantitative or qualitative triggers based on multiple sources of information for early identification of potentially harmful scenarios. They have the following characteristics:

- **Rule based triggers -** These are triggers to flag risks early based on rules – that can be quantitative (like sharp increase in resource cost) or qualitative (like impact on brand/ reputation).
- **Multiple sources of information -** The triggers could be based on internal information such as supplies, labour issues, high attrition etc. or external information such as changes in travel regulations, macro-economic developments etc.

To manage risks effectively, it is important to monitor them regularly. Early warning indicators are set up using the following key parameters:

- **Reporting frequency:** How often risk information and updates are reported.
- **Threshold:** The level at which a risk requires attention or action.
- **Risk appetite:** The amount of risk the organization is willing to accept.
- **Actual value:** The current measured value of a risk indicator.

3.1.4. Step 4: Monitor Risks

Monitoring is performed at multiple levels to ensure that risk management continues to be applied within the company.

- **Risk Owners**: Risk owner shall be the first person responsible for monitoring risks related to their function or span or specially assigned to them. Risk owners shall review and report the status of the major risks and mitigation plan actions to the Risk Officer on a **biannual** basis. The Risk Officer shall consolidate and present these updates to the Risk Management Committee (RMC) at its scheduled meetings.
- **Board**: Board shall meet and discuss risks at least on an annual basis. The objectives of these meetings shall be as follows:

    - Identify any new enterprise risks that may have emerged.
    - Assess notable change in risk rating of identified risks (impact or probability).
    - Measures undertaken by the company to mitigate identified business risks.
    - Review status of implementation of mitigation plans.
    - Establish whether actions have been completed or are on target for completion.

3.1.5. Step 5: Reporting

A structured reporting cadence ensures that information flows efficiently from operational units to the Board, ensuring no critical threat goes unnoticed.

- Risk Register: The Central Risk Register is maintained by the Risk Officer and is updated on a biannual basis, with a comprehensive review at least annually.
- Risk Management Committee (RMC): Meets bi-annually to review the Top 10 Risk Mitigation Plans and the overall efficacy of the Risk Management Framework. The Committee reviews management's approach and provides specific suggestions to strengthen controls.
- Board of Directors: Conducts an annual review of the overall Risk Management Framework to ensure it remains aligned with the Company's strategic objectives.

3.2. Risk Workshop

Risk management workshops are planned as a core component of its enterprise risk management process. These workshops are designed to facilitate informed decision-making, foster cross-functional collaboration, and ensure that enterprise risks are systematically identified, assessed, prioritized, and addressed. The workshop program is structured across two sequential sessions, each serving a distinct purpose in the risk management lifecycle.

Workshop 1 — Risk Identification and Prioritization

The first workshop focuses on establishing a shared understanding of the enterprise risk landscape. The session commences with a presentation of the pre-workshop survey results, providing participants with a data-driven foundation for discussion. Facilitators then lead a structured review of the top-ranked risks identified through the survey, enabling stakeholders to assess each risk in the context of the organization's strategic objectives. Group discussions are held to evaluate the significance of each risk, considering factors such as likelihood, potential impact, and velocity of onset.

Following these deliberations, participants collectively prioritize enterprise risks using agreed-upon scoring criteria and confirm risk ownership for each identified risk domain. The session concludes with an initial discussion of potential response approaches. Following the workshop, assigned risk owners are responsible for further assessing their respective risks and developing proposed mitigation strategies, detailed action plans, action owners, implementation timelines, and Key Risk Indicators (KRIs) for presentation and review in the subsequent workshop.

Workshop 2 — Risk Response and Register Foundation

The second workshop builds upon the outcomes of the first session and focuses on finalizing risk treatment decisions and establishing the foundation of the Enterprise Risk Register. The session begins with confirmation of the shortlist of priority risks requiring active management and ongoing monitoring.

Risk owners present their proposed mitigation strategies, response actions, assigned action owners, implementation timelines, and KRIs for each priority risk. Participants review, challenge, and refine these proposals to ensure alignment with business objectives, risk appetite, and operational realities. Risk priority assessments are validated during this session to confirm consistency and objectivity across all assessed risks.

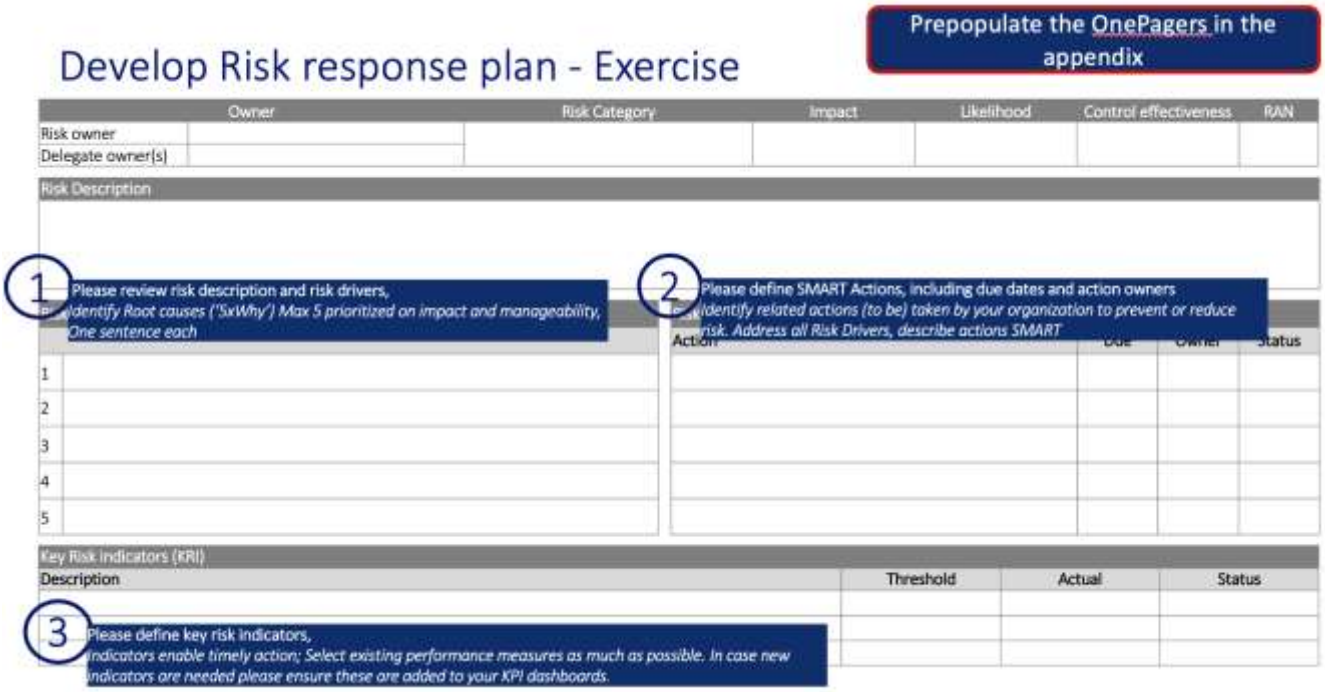
Following discussion, stakeholders formally agree on the final response strategies, mitigation actions, ownership responsibilities, and monitoring mechanisms for each priority risk. The session concludes with the consolidation of all agreed risk information, including risk descriptions, ratings, owners, response plans, KRIs, and action tracking details into the initial Enterprise Risk Register, establishing the organization's authoritative record for ongoing risk governance and oversight.

4. Annexure

4.1. Risk Register & Mitigation Template

This section will have the current risk register of the Company along with the mitigating measures. Illustrative templates are as follows:

Risk Mitigation Template:



Risk Register as per suggested policy:

#	Risk Category	Risk	Risk Description	Risk Impact	Risk Likelihood	Risk Score	Overall Risk Grade (L/M/H)	Risk Owner	Risk Mitigation Plan	Action Plan Target Date	Action Plan Status	Remarks