OPERATIONAL RISK AND OPERATIONAL RESILIENCE DOCUMENT OF LENDINGKART FINANCE LIMITED
(Last Updated – November 2025)

Contents

1. Background

Lendingkart Finance Limited (‘**LFL’ / ‘Company’**) is engaged in the business of providing term loans to micro, small and medium enterprises. LFL is a non-deposit taking NBFC which falls under the middle layer as per RBI guidelines on scale-based regulations.

Operational Risk is a complex risk category, when it comes to identification, quantification and mitigation of risk. It is impacted by numerous factors such as internal business processes, regulatory landscape, business growth, customer preferences, and even factors external to an organization. Therefore, LFL has formulated this Operational Risk Management Framework (ORMF).

This ORMF has been built on three pillars. The three pillars are:

(i) Prepare and Protect
(ii) Build Resilience
(iii) Learn and Adapt

These three pillars support a holistic approach to the management of Operational Risk and Operational Resilience and create a feedback loop that fosters perpetual embedding of lessons learned into LFL’s preparation for operational disruptions and its performance during actual occurrence of disruptions.

Objectives of the Framework

The objectives of the ORMF include:

- To proactively manage Operational Risk excluding Strategy, Reputational risks.
- To establish a governance structure that will be responsible for effective Operational Risk management across the organisation.
- To conduct appropriate training to staff and senior leadership at LFL on the significance and mechanisms of Operational Risk management.
- To appropriately establish, maintain and review procedures at management and operational level to identify, monitor and mitigate Operational Risk in accordance with the company's risk management framework. To ensure Operational Resilience through effective Operational Risk Management by integration of dependencies of systems and third-party vendors.

PILLAR I: Prepare and Protect

2. Three lines of defence for management of Operational Risk

a. First line of defence

The first line of defence will be Business functions and operations including Information Technology function. These functions carry out various activities which are directly related to business such as sourcing, credit underwriting, operations, loan disbursal, accounting, Information technology support etc. First line of defence are the owners of risk and responsible to identify, assess, mitigate and monitor risks.

Sound Operational Risk governance recognises that business unit management is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is accountable.

b. Second line of defence

i. The second line of defence which will support the first line of defence in identification, assessment, mitigation and monitoring of risks. Functionally independent Organisational Operational Risk Management Department (ORMD) forms the second line of defence along with the Compliance function.

ii. The responsibilities of the second line of defence in promoting a sound Operational Risk Management culture includes:

(i) Developing an independent view regarding business units' (a) identified material Operational Risks, (b) design and effectiveness of key controls, and (c) risk appetite and risk tolerance as defined in risk appetite statement of the Organization which is reviewed and approved by the Board.
(ii) Challenging the relevance and consistency of the business unit's implementation of the Operational Risk Management tools, measurement activities and reporting systems, and providing evidence of this effective challenge.
(iii) Developing and maintaining Operational Risk Management policy and standard operating procedures (SOP)
(iv) Reviewing and contributing to the monitoring and reporting of the Operational Risk profile carried out by the identified first line of defence and
(v) Designing and providing Operational Risk training and instilling risk awareness. Details of all such training need to be kept on record.

c. Third line of defence

The third line of defence, i.e the audit function provides an independent assurance to the Board regarding the appropriateness of LFL's ORMF. This function's staff is not involved in the development, implementation and operation of Operational Risk Management processes which has been carried out by the other two lines of defence. The third line of defence reviews are carried out by LFL's internal and/or external audit but may also involve suitably qualified independent third parties.

i. Such audits shall be conducted every year in line with the approved annual audit plan.

ii. An effective independent review with risk based Internal audit approach includes two processes:

   i. **Validation:** The audit function shall ensure that the quantification systems used by LFL are sufficiently robust as (i) they provide assurance about the integrity of inputs, assumptions, processes and methodologies and (ii) results in assessment of Operational Risk that credibly reflects the Operational Risk profile of LFL.

   ii. **Verification:** In this process, the audit function shall undertake-

      a. Review of the design and implementation of the Operational Risk Management processes (including compliance and consistency with Board policies) through the first and second lines of defence (including the independence of the second line of defence).
      b. Review of validation processes to ensure they are independent and implemented in a manner consistent with established LFL policies
      c. Ensuring that business units' management promptly, accurately and adequately responds to the issues raised, and regularly reports to the Board of Directors or its relevant Committees on pending and closed issues
      d. Identifying gaps, if any, in the ORMF and reporting to the Board or its relevant Committees; and
      e. Providing opinion on the overall adequacy and appropriateness of the ORMF and the associated governance processes across the RE by assessing whether the ORMF meets organisational needs and expectations (such as in respect of the risk appetite and tolerance, and adjustment of the framework to changing circumstances) and complies with statutory and legislative provisions, contractual arrangements, internal rules and ethical conduct.

d. Conclusion on 3 lines of defence

i. LFL ensures that each line of defence

   i. Has clearly defined roles and responsibilities.
   ii. Is adequately resourced in terms of budget, staff and tools.
   iii. Is continuous and adequately trained.
   iv. Promotes a sound Operational Risk management culture across the organisation.
   v. Communicates with the other lines of defence to reinforce the ORMF.

3. Governance and Risk Culture

i. LFL has constituted the Operational Risk Executive Committee (OREC) as a Management Committee which works with the Board of Directors and Senior Management and will supervise the workings of the 3 lines of defence mentioned above. The governance structure for the purpose of sound Operational Risk management is as under:

   i. Board of Directors: The Board is ultimately responsible and accountable for oversight of Operational Risk Management.
   ii. Risk Oversight Committee (ROC): The ROC is responsible for evaluating the overall risks faced by the company including liquidity risk and shall report to the Board.
   iii. Operational Risk Executive Committee (OREC): The OREC is responsible for establishing, maintaining and reviewing procedures at management and operational level.
   iv. Senior Management: Senior management are responsible for management and ownership of Operational Risk across LFL's end-to-end processes.

ii. The actions of the Board of Directors and Senior Management as well as the LFL's risk management policies, processes and systems provide the foundation for a sound risk management culture. In this context, the Board of Directors has duly formulated a 'Code of conduct'/ 'Ethics Policy' to address conduct risk. The policy is applicable to all staff and Board members of LFL and inter alia, outlines the expectations for integrity and ethical values, acceptable business practices and accountabilities.

4. Responsibilities of Board of Directors and Senior Management

a. Responsibilities of Board of Directors

1. Review and approve ORMF as and when necessary, and ensure that Senior Management implements the policies, processes and systems of the ORMF.
2. Establish a risk management culture and ensure that LFL has adequate processes for understanding the nature and scope of the Operational Risk inherent in its current and planned strategies and activities.
3. Ensure that the Operational Risk Management processes are subject to comprehensive and dynamic oversight and are fully integrated into, or coordinated with, the overall framework for managing all risks across the Organization.
4. Provide senior management with clear guidance regarding the principles underlying the ORMF, and approve the corresponding policies developed by senior management to align with these principles.
5. Regularly review and evaluate the effectiveness of and approve the ORMF to ensure the LFL has identified and is managing the Operational Risk arising from external market changes and other environmental factors, as well as those Operational Risks associated with new products, services, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes).
6. Ensure that the LFL's ORMF is subject to effective independent review by a third line of defence (audit or other appropriately trained independent third parties from external sources).

7. Take active role in establishing a broad understanding of the LFL's Operational Resilience approach, through clear communication of its objectives to all relevant parties, including the LFL's personnel, third parties, and intragroup entities.
8. Establish clear lines of management responsibility and accountability for implementing a strong control environment. Controls should be regularly reviewed, monitored, and tested to ensure its ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between Operational Risk Management functions, business units and support functions.
9. Review and approve LFL's Operational Resilience approach considering the LFL's risk appetite and tolerance for disruption to its critical operations. In formulating the LFL's tolerance for disruption, the Board of Directors should consider its operational capabilities given a broad range of severe but plausible scenarios that would affect its critical operations. The Board of Directors should ensure that LFL's policies effectively address instances where its capabilities are insufficient to meet its stated tolerance for disruption
10. The risk appetite and tolerance statement for Operational Risk should be developed under the authority of the Board of Directors and linked to the LFL's short and long-term strategic and financial plans. Taking into account the interests of the 's customers and stakeholders as well as regulatory requirements, an effective risk appetite and tolerance statement should:

- Be easy to communicate and easy to understand for all stakeholders
- Include key background information and assumptions that informed LFL's business plans at the time of its approval
- Include statements that clearly articulate the motivation(s) for taking on or avoiding certain types of risk, and establish boundaries or indicators (which may be quantitative or not) to enable monitoring of these risks
- Ensure that the strategy and risk limits of business units and legal entities, as relevant, align with the LFL-wide risk appetite statement; and
- Be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the Organization understands what events might push it outside its risk appetite and tolerance statement

11. Approve the set-out criteria for defining its critical operations and tolerances. The criteria should account for factors such as the potential risk to:

- Customers: The impact on customers' services, transactions, and relationships.
- Viability: How the operation impacts financial and operational health.
- Safety and Soundness: Ensuring that essential functions are preserved to maintain regulatory compliance and business continuity.
- Financial Stability: Minimizing disruptions that could undermine LFL's financial position or reputation.

The criteria for the identification of critical operations should be reviewed and approved by the Board annually or at the time of implementing material changes to the business that would involve additional critical operations.

The criteria for defining impact tolerances include:

- Documenting all processes including dependent systems and third-party vendors
- Defining RTO (recovery time objectives) and RPO(recovery point objectives) for each process
- Assessing financial, operational, legal and reputational impact of each process
- During Business Impact Assessment (BIA), critical processes are identified and mapped to Operational Risk for assessment. BIA is governed by a separate Policy on BCP. The Information Technology -department is the owner of BCP.

12. Review and approve impact tolerances for each critical operation at least annually or as and when a disruption occurs. The purpose of impact tolerance is to quantify the maximum acceptable level of disruption for each critical operation. It needs to be tested against severe but plausible scenarios to

determine their appropriateness, i.e., to determine whether LFL is able to stay within the defined impact tolerances during a disruption.

b. Responsibilities of Senior Management

1. Translate the ORMF approved by the Board of Directors into specific policies and procedures that can be implemented and verified within the different business units. It should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure the necessary resources are available to manage Operational Risk in line with LFL's risk appetite and tolerance statement. Moreover, it should also ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.
2. Establish and maintain robust challenge mechanisms and effective issue resolution processes. These should include systems to report, track, and when necessary, escalate issues to ensure resolution. LFL should be able to demonstrate that the three-lines-of-defence approach is operating satisfactorily and to explain how the Board of Directors, independent Audit Committee of the Board, and Senior Management ensure that this approach is implemented and operating in an appropriate manner
3. Ensure that staff responsible for managing Operational Risk co-ordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in LFL who are responsible for the procurement of external services such as insurance risk transfer and other third-party arrangements. Failure to do so could result in significant gaps or overlaps in LFL's overall risk management programme.
4. Be of sufficient stature to perform their duties effectively, ideally evidenced by a title that is commensurate with other risk management functions such as credit, market and liquidity risk.
5. Ensure that LFL's activities are conducted by staff with the necessary experience, technical capabilities and access to resources. The staff responsible for monitoring and enforcing compliance with LFL's risk policy should have authority independent from the units they oversee.
6. Ensure that LFL's policies, processes and systems under ORMF remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner.
7. Ensure that LFL's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence.
8. Implement a process to regularly monitor Operational Risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the Board of Directors, Senior Management, and business unit levels to support proactive management of Operational Risk.
9. Senior Management should provide timely reports to the Board on the ongoing operational resilience of the LFL's business units to support the Board's oversight, particularly when significant deficiencies could affect the delivery of the RE's critical operations.

5. Risk management environment - Identification and assessment

- Risk identification and assessment are fundamental characteristics of an effective Operational Risk Management system and directly contribute to Operational Resilience capabilities. Effective risk identification considers both internal and external factors. Sound risk assessment allows LFL to better understand its risk profile and allocate risk management resources and strategies most effectively. Results of the LFL's Operational Risk assessment should be incorporated into overall business strategy development process.
- LFL has employed the following tools for identifying and assessing Operational Risk: Detailed guidelines of these tools are provided in the Operational Risk SOP.

  i. **Self-assessments –** Each business unit at the first line of defence shall perform self-assessments of their respective Operational Risks and controls at various levels which typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered) and contain both quantitative (such as metrics, benchmarking, etc.) and qualitative (such as likelihood and consequence of the risk event in determination of inherent and residual risk ratings) elements.

ii. **Operational Risk event data –** LFL shall maintain a comprehensive Operational Risk event dataset that collects all material events experienced by the LFL and serves as the basis for Operational Risk assessments. The event dataset typically includes internal loss data, near misses, etc., and is classified according to a taxonomy defined in the ORMF policies and consistently applied across the LFL.

iii. **Event management –** LFL will conduct an analysis of events to identify new Operational Risks, understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events

iv. **Control monitoring and assurance framework –** LFL shall adopt an appropriate control monitoring and assurance framework that facilitates a structured approach to the evaluation, review and ongoing monitoring and testing of key controls.

v. **Metrics –** LFL shall develop key risk indicators and linkage with associated risk and controls to assess and monitor their Operational Risk exposure.

vi. **Scenario analysis –** LFL shall consider internal and external loss data, information from self-assessments, the control monitoring and assurance framework, forward-looking metrics, root-cause analyses and the process framework. Scenario analysis is a method to identify, measure and analyse a range of scenarios, including low probability and high severity events, some of which could result in severe Operational Risk losses.

vii. **Benchmarking and comparative analysis –** Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within

LFL, as well as comparisons of metrics of the LFL, with other regulated entities in the industry. Such comparisons can be performed to enhance understanding of the LFL's Operational Risk profile.

6. Change management

Defining the Change Process: To build a process that could identify, track and resolve changes impacting business processes - these changes could be either driven externally (because of regulation/policy changes, co-lender requirements, other market conditions) or internally (strategic directioning, new developments, bug fixes etc.)

- Any new Product/s or significant change/s to the existing Product will be reviewed and approved by the Product Approval Committee (PAC).

- Any notable change/s in IT (Information Technology) or IT Systems will be reviewed and approved by the Information Technology Steering Committee (ITSC).

- Business process related changes shall be reviewed by the Operational Risk Management department in conjunction with the Business team and approved by the Head of Department. All approved process related changes are duly incorporated in the Standard Operating Procedure (SOP).

7. Monitoring and reporting

- Appropriate reporting mechanisms should be in place at the Board of Directors, Senior Management, and business unit levels to support proactive management of Operational Risk.
- Reports on Operational Risks should be comprehensive (covering all relevant areas), accurate (correct data), consistent (standardized and comparable), and actionable (useful for decision-making) across business units and products.
- Types of reports at all levels of LFL governance to support proactive management of Operational Risk include (Not limited to):

i. Significant Operational Risk Events (SORE)
ii. Operational loss incidents (if any)
iii. Update on frauds
iv. Update on information security
v. Update on Compliance related aspects
vi. Overdue IAD observations
vii. Operational Risk KRIs
viii. Update on RCSA

Any other items that are not listed above as required.

8. Control and mitigation

- **Risk and compliance assessment**

i. Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws. Examples of principal elements of a policy compliance assessment are:
a. Top-level reviews of progress towards stated objectives
b. Verification of compliance with management controls
c. Review of the treatment and resolution of instances of non-compliance
d. Evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management

ii. Tracking of reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy, regulations and laws. Each function has documented SOP on their processes which should be adhered to. These SOPs cover all controls that are required to mitigate risks.
iii. Operational Risk SOP provides details of risk assessment, identification, mitigation and reporting of Operational Risks.

- **Control processes and procedures**

i. Clearly established authorities and/or processes for approval
ii. Close monitoring of adherence to assigned risk thresholds or limits
iii. Safeguards for access to, and use of, RE assets and records iv. Appropriateness of staffing level and training to maintain technical expertise
v. Ongoing processes to identify business units or products where returns appear to be out of line with reasonable expectations.
vi. Regular verification and reconciliation of transactions and accounts

- **Approach to identifying, measuring, monitoring and managing technology risks**

i. Same ORM framework and tools are used to identify, measure, monitor and manage technology risks.
ii. ORM department shall take support of Information Security department for this activity till capability is built within ORMD,
iii. RCSA of Information Technology function shall be carried out annually or as prescribed and KRIs of IT functions shall be monitored regularly.
iv. There is a separate Board approved Information security policy to manage Information and Cyber security for the Organization.
v. The use of technology related products, services, activities, processes and delivery channels exposes the Organization to Operational Risk and the possibility of material financial loss.

Consequently, LFL should have an integrated approach to identifying, measuring, monitoring and managing technology risks along the same precepts as Operational Risk Management

PILLAR 2: Build Resilience

9. Mapping of Interconnections and Interdependencies

- **Mapping Critical Operations and Dependencies**

i. LFL must identify and document all key elements—people, technology, processes, information, facilities—that are necessary to deliver their critical operations. This includes understanding how these elements depend on third-party providers or arrangements within the group (intragroup dependencies). The purpose of this mapping is to understand the scope and complexity of the Operational Resilience.

ii. This mapping is carried out post completion of Business Impact Assessment (BIA) as part of BCP. There is a separate Board approved BCP policy in place.

- **Granularity of Mapping and Identifying Vulnerabilities**

The mapping should be detailed enough to help LFL identify vulnerabilities and assess their ability to maintain critical operations under disruption. The mapping should consider various risks such as Reputational, Legal, Financial, Compliance and Operational Risks.

10. Third-party dependency management

LFL has a Board approved Outsourcing risk policy and IT services outsourcing policy to manage third party dependency for critical operations. In addition to onboarding due diligence by the onboarding department, Operational Risk also carries out annual risk assessment of material vendors to ensure resilience in line with agreed terms. For non-material vendors review will be performed as and when required based on change of scope of services, at least once every 3 years.

11. Business Continuity Planning and Testing

LFL has a Board approved BCP policy covering key activities like BIA, BCP testing, DR framework, alignment with recovery plans, periodic testing of BCP etc.

12. Information and Communication Technology (ICT) including Cyber Security Framework

LFL has Board approved Information and Cybersecurity policy and BCP policies to manage ICT and Business continuity risk. Governance and roles & responsibilities of senior management are clearly mentioned in those policies including management level and Board level committees for oversight of risks.

PILLAR 3: Learn and Adapt

13. Disclosure and reporting

The Operational Risk department shall disclose below information to internal and Board level committees

i. Public Disclosure for Transparency and Market Discipline

ii. Significant Operational Risk Events (SORE) with causes, impact, and lessons learned. This enables stakeholders to understand LFL's experience with Operational Risks and its capacity to recover and improve. Loss events should be contextualized to avoid unnecessary panic and to give stakeholders a full understanding of the operational environment.

iii. Operational losses including fraud losses iv. Key risk indicators (KRI)

v. Update on RCSA
vi. Update on open internal audit observations
vii. Update on compliance related risks. viii. Update on Information Security related risks
ix. Update on reported and attempted frauds including fraud loss booked and recovery.
x. Any other information as required from time to time. Complete details of disclosures and reporting are mentioned in the Operational Risk SOP.

14. Lessons Learned Exercise and Adapting

- LFL should conduct a ‘lessons learned exercise’ on a need basis including Root Cause Analysis, after any disruption to a business service with emphasis on critical service. This includes any potential material disruption to a third-party provider (including but not limited to a group entity) that feeds into the delivery of a critical business service. The lessons learned exercise should utilise the information gathered as part of the incident management and disaster recovery process.

15. Continuous improvement through Feedback Systems

- Continuous improvements to Operational Resilience require LFL to learn from its experiences as changes to its operational approaches or technology infrastructure mature over time. This should not only occur after a disruption or incident has occurred but should form part of ongoing Operational Resilience discussions.

- LFL should promote an effective culture of learning and continuous improvement as Operational Resilience evolves. Operational Resilience needs to be a fundamental element of any strategic decision taken by the Organization.

- LFL should develop robust feedback systems to ensure a continuous positive feedback loop fostering an effective learning environment, which in turn helps them frame better ORMFs and build adequate Operational Resilience

*** End of Document ***

Glossary:

- ORMD - Operational Risk Management Department
- ORMF – Operational Risk Management Framework
- RCSA – Risk & Controls Self-Assessment
- KRI – Key Risk Indicators
- OREC – Operational Risk Executive Committee
- SORE – Significant Operational Risk Event
- ICT – Information and Communication Technology
- TOR – Terms of Reference
- CMC – Change Management Committee
- BCP – Business Continuity Plan
- BIA – Business Impact Assessment
- SOP – Standard Operating Procedure
- IAD – Internal Audit Department
- LFL – Lendingkart Finance Limited