KIFS Housing Finance Limited

OPERATIONAL RISK DISCLOUSURE POLICY

Version 1.0

Disclaimer: *This document contains material classified "Confidential". Except as specifically authorized by KIFS the holder of this document shall keep the information contained herein confidential and shall protect the same in whole or in part from disclosure or dissemination to any unauthorized party.*

Version	Prepared by	Reviewed by	Approved by	Approved Date
1.0	Gayatri Rane – Policy Manager	Sandeep Verma – Operations Head	Board	September 15, 2025

Index

Chapter 1: Introduction

This policy represents a thorough and detailed disclosure of the operational risk exposures and the operational risk management framework of KIFS. By presenting this information, the policy aims to provide stakeholders with a comprehensive understanding of the approach adopted to manage operational risks and exposures. Ultimately, the policy serves as a valuable tool for stakeholders to assess KIFS's resilience in delivering critical operations during disruptions and to determine whether KIFS effectively identifies, assesses, monitors, and controls or mitigates operational risk.

Chapter 2:

Scope & Objectives

This policy governs the identification, assessment, and disclosure of operational risk-related information, ensuring that:

- The disclosures provide a clear understanding of KIFS operational risk framework.
- The disclosed information is accurate, complete, and reliable.
- KIFS meets regulatory and compliance requirements.

Chapter 3: Overview of Operational Risk

Operational risk is inherent in all financial products, activities, processes, and systems. Operational risk is defined as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition includes legal risk but excludes strategic and reputational risk. Where appropriate, strategic and reputational risks should be taken into consideration under the Operational Risk Management Framework ("ORMF").

The increasing scope and complexity of products and services, processes, and systems, and changing external environment have made KIFS's risk profile more sophisticated. Failure to responsibly manage operational risk may bring significant losses to KIFS. As such, KIFS has developed its ORMF to promote a proactive and consistent operational risk culture on a continuous basis to address the ever-changing operational risk landscape and ensure its long-term sustainability. The ORMF provides the standards and guidelines to identify, measure, monitor, and control or mitigate operational risk in relation to KIFS's daily

activities. It defines the environment and organizational components for managing operational risk in a structured systemic and consistent manner to align with the company's risk appetite, as well as the related risk policies and procedures outlining roles and responsibilities, data standards, risk assessment processes and methodology, and reporting standards.

Chapter 4: Disclosure Determination Process

KIFS adopts a structured approach to determining operational risk disclosures based on the following:

- Materiality and relevance of operational risk incidents.
- Impact on financial performance, reputation, and regulatory standing.
- Regulatory and industry best practices.
- Stakeholder expectations.

Key Risk Indicators:

Key risk indicators (KRIs) allow for the monitoring of operational risks through defined metrics. Examples of KRIs include:

Sr. no	Metric	Computation (Impact)	Significant	Major (Risk Tolerance)	Moderate (Risk Appetite)	Minor	Negligible
1	Max. operational losses (% of operating profit)	Computed as total operational losses / Pre-provision operating profit	>5%	<5%	<2%	<1%	0.00%
2	Max. percentage where repayment (NACH / e-NACH) instrument is not available	% of cases where NACH/e-NACH is not activated vs No. of cases disbursed	>10%	<10%	<7.5%	<5%	0%
3	Max. percentage where Officially Valid Documents ("OVD") are pending	% of OVD Document outstanding >90 days for total active customers (regulatory breach)	>10%	<10%	<7.5%	<5%	0%

4	Number of instances of non-receipt of collateral documents leading to unsecured loans	% of loan exposure with documents pendency/Total Loan Book	>10%	<10%	<7.5%	<5%	0%
5	Number of instances where periodic updation of KYC not carried out at the required intervals	% of loan exposure wherein Re-KYC is pending/Total Loan Book	>2%	<2%	<1.5%	<1%	0%
6	Number of instances where CKYC ID is not generated for the disbursed case	% of loan exposure wherein CKYC is pending/Total Loan Book	>2%	<2%	<1.5%	<1%	0%
7	Instances of loan amount disbursed in excess of the sanctioned loan amount	% of Loan Disbursed in excess / Total Disbursement	>2%	<2%	<1.5%	<1%	0%
8	Instances of collection of cash by the employee but delay in deposition(3 Working days)	Total of cash delayed deposition / total collection pool	>2%	<2%	<1.5%	<1%	0%
9	PDCs exhausted OPS	To analyze those loans where the Post-Dated Cheques for instalments have exhausted, which can lead to an increase in debtors.	>10%	<10%	<7.5%	<5%	0%
10	Forged cases of Credit	This indicator points the case where the forged documents were provided for the loan appraisal. The company has internal verification/external verification system to identify these cases and the he cases are identified prior to sanction/disbursement.	>5%	<5%	<3%	<1%	0%

11	Improper Documentation	No. of Instances in which Company suffered loss due to inadequate and incomplete documentation during disbursement of loan. If the documents are partially / wrongly filled, our legal position may be weak in case we have pursued litigation.	>5%	<5%	<3%	<1%	0%
12	Infringement HR	An act of burglary, theft, etc. in the office premise	>5	<5	<3	<1	<1
13	Contracts Expired	The annual contracts and lease deeds expired but Not renewed on time	>10%	<10%	<7.5%	<5%	0%
14	Declined cases	This indicator depicts the quality of log-ins as decline cases to total log- ins	>10%	<10%	<7.5%	<5%	0%
15	Stale entries	No. of entries in suspense accounts (sundry debtors) outstanding for more than three months	>10%	<10%	<7.5%	<5%	0%
16	Un- reconcile d Debit bank Entries	No. of entries in bank accounts Not reconciled for more than three months	>10%	<10%	<7.5%	<5%	0%
17	Data rejection by CIC (DQR - Data Quality report)						

Chapter 5: Three Lines of Defense

KIFS's risk governance framework provides clear oversight and ownership of management of operational risk across three lines of defense. The first line of defense comprises business lines and operational functions whereas the second and third lines of defense involve independent risk

management and control functions.

Defense	Role
First Line of Defense – Lines of Business	Owns and manages operational risk.
Second Line of Defense – Independent Risk Management and Control Functions	Oversees and monitors operational risk.
Third Line of Defense – Internal Audit and Loan Review	Provides independent assurance of Management's adherence to approved policies and regulations. Conducts audits and reviews.

Chapter 6: Risk Management Process

KIFS has established a mechanism to manage and control operational risk effectively according to the regulatory guidance and the KIFS policies. KIFS's operational risk management process incorporates the end-to-end approach of managing operational risk at various stages. KIFS has formulated effective means to regularly identify, assess, monitor, and control the operational risk inherent in its products, activities, processes, and systems in a timely manner.

KIFS reviews and enhances the granularity of assessments to evaluate the quality and appropriateness of corrective and mitigation actions and ensures that adequate controls and systems are in place to identify and address problems before they become major concerns.

The following table is a description of KIFS's operational risk management process:

Process	Description
Risk Identification and Assessment	Several tools are used for identifying and assessing operational risk inherent in existing or new products and services, business activities, operational processes, and systems, including but not limited to, event management, operational risk event data analysis, self-assessment, control monitoring and testing, monitoring risk metrics, etc.

Risk Monitoring and Reporting	KIFS has a risk monitoring and reporting process to monitor its operational risk profile and material exposure to operational losses on an on-going basis. The process includes both qualitative and quantitative assessments of KIFS's exposures to key types of operational risks to identify and address problems before they become major concerns. Key operational risk indicators and metrics are implemented to assess and measure the operational risk profile of individual functional department or unit, and that of KIFS. KIFS's ORMF has tools for systematically tracking and recording loss data, especially on its frequency, severity, and other relevant information on loss events. Risk reports, which contain the following types of information, including but not limited to operational risk events, results and analysis of operational risk metrics, Risk and Control Self- assessment ("RCSA") results, internal audit findings, etc., are regularly submitted to senior management for review and oversight.
Risk Control and Mitigation	KIFS has risk management measures to control and mitigate operational risk. Such measures include risk assessment, activities monitoring and control, communication and information sharing, training, establishment of departmental procedures, business continuity and disaster recovery planning, and insurance to cover possible losses resulted from operational incidents.

Chapter 7: Operational Risk Management Strategy

KIFS's operational risk management begins with the determination of the overall risk management strategies defined by the Risk Management Committee including, but not limited to, risk appetite or

tolerance, and ensures that the defined strategy aligns with the overall business objectives and risk management process.

KIFS places significant emphasis on operational risk management in its current strategy development process, encourages clear understanding and effective communication, and establishes a process to define and document relevant operational risks, their root causes and lessons learnt to strengthen its resiliency towards operational risk and disruptions.

KIFS keeps on effectively implementing strategies on operational risk management, where appropriate, organizational structures, business processes, compensation systems, and resource availability need to be considered to ensure that operational risk management strategies are integrated into KIFS's daily operational activities and business development.

Chapter 8: Operational Risk Management Tools

To measure and manage operational risk effectively, KIFS uses the following tools to regularly monitor and assess its operational risk profile:

1. **RCSA**

   RCSA is a structured approach adopted by all functional departments or units at KIFS to assess their risk exposure and control environment. It involves implementing specific action plans to address identified risks, ensuring that business objectives are pursued in a risk-controlled manner. RCSA is used to proactively identify, assess, monitor, and control or mitigate operational risks inherent in work processes. It also provides a robust and consistent framework for reviewing the adequacy and effectiveness of existing controls.

2. **Key Risk Indicators ("KRIs") and Metrics**

   KRIs provide quantitative insights into KIFS's operational risk exposure and the effectiveness of its control environment. Metrics serve as management thresholds to monitor major risk factors that could cause business disruptions, operational losses, reputational damage, financial crimes, regulatory non-compliance, or conduct issues. KRIs and metrics play a preventative role by helping identify trends and warning signs, offering valuable inputs for management decision-making.

3. **Residual Risk Assessment**

   Residual risk refers to the level of risk that remains after risk controls have been applied to a given process or event. If residual risk is rated as "High" or "Medium," the designated risk owner must assess the situation, perform a business impact analysis, and propose alternative mitigation actions for the Risk Management Committee (RMC) to consider.

4. **Operational Risk Event Data**

   KIFS maintains a comprehensive dataset of operational risk events, encompassing both quantitative and qualitative details of internal and external incidents. The dataset supports ongoing risk assessments and includes information on root causes and control deficiencies. This analysis fosters knowledge sharing and enables departments to learn from past events—

especially recurring ones—across the organization.

5. **Incident Reporting Process**

   The incident reporting and escalation process is designed to capture and analyze operational risk incidents, derive lessons learned, and take corrective action. Significant incidents are escalated promptly to senior management, and their impacts are thoroughly assessed to close any operational risk management gaps.

6. **Products, Services and Vendor List**

   To assess risk changes stemming from product, service, or vendor modifications, KIFS maintains a centralized record of all products, services, and outsourced functions. This registry supports risk assessments during change initiatives and facilitates effective monitoring of evolving operational risks.

Operational Risk Points Identified in Each Tool:

Tool	Operational Risk Points Addressed
RCSA	Internal process risks, control weaknesses, manual errors, accountability gaps.
KRIs and Metrics	Early warning signals for potential operational failures, fraud, compliance issues, and system breakdowns.
Residual Risk Assessment	Effectiveness of control implementation, high-risk areas that may lead to financial loss or regulatory impact.
Operational Risk Event Data	Lessons from past incidents, recurring failures, root cause analysis, systemic vulnerabilities.
Incident Reporting Process	Real-time operational disruptions, escalations, and

	oversight of high-severity events.
Products/Services/Vendor List	Risks from new initiatives, third-party/vendor failures, changes in process or service delivery, and outsourcing risks.

Chapter 9: Risk Response Process

After the operational risk management process, KIFS evaluates the situation and chooses from the following alternative actions to respond to the identified risks:

Action	Description
Risk Mitigation	Reduce or eliminate risk through implementation of controls, or develop and implement mitigation action plans.
Risk Transfer	Transfer the risk partially or in full to a third-party (such as insurance coverage), or another business sector or area, or create a new risk (such as legal or counterparty risk).
Risk Avoidance	Develop and implement actions to avoid the risk.
Risk Acceptance	Decide to accept the risk and consequences within the Company's risk appetite and tolerance with risk acceptance approval in accordance with the Company's policies.

Chapter 10: Internal Controls

To ensure accuracy and reliability, KIFS implements robust internal controls, including:

- A designated team responsible for compiling, verifying, and approving disclosures.
- Cross-functional review mechanisms to validate the authenticity of disclosed data.
- Secure documentation and reporting channels to prevent unauthorized access or manipulation.

Chapter 11: Regular Review & Assessment

KIFS shall periodically assess the appropriateness of its operational risk disclosures through:

- Annual reviews by Senior Management and Risk Committees.
- Independent audits or assessments to evaluate compliance and effectiveness.
- Continuous monitoring and feedback mechanisms to refine disclosure practices.

Chapter 12: Policy Review

This policy shall be reviewed at least annually or as required to reflect changes in regulatory frameworks, industry practices, or internal operational risk management strategies.