Technical Guide on Risk Based Internal Audit of Non-Banking Financial Company (NBFC)

Board of Internal Audit and Management Accounting
The Institute of Chartered Accountants of India
(*Set up by an Act of Parliament*)
New Delhi

Basic draft of this publication was prepared by CA. Deepti Rathor and CA. Bharat Ramani.

First Edition	:	May, 2024
Committee/Department	:	Board of Internal Audit and Management Accounting
E-mail	:	biama@icai.in
Website	:	www.icai.org/ www.internalaudit.icai.org
Price	:	₹ 200/-
ISBN	:	978-81-19472-57-4
Published by	:	The Publication & CDS Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002 (India)
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra - 282 003 June | 2024 | P3661 (New)

Foreword

Non-Banking Financial Companies (NBFCs) contribute to the economic and social development of India by promoting inclusive growth and catering to the diverse financial needs of the population. As on 30th September 2023, there were 9,356 NBFCs and 27 Asset Reconstruction Companies (ARCs) registered with Reserve Bank of India (RBI).

As NBFCs are empowering small businesses by offering a wide array of financial services, thus it requires disciplined environment through internal audit system. The RBI has mandated Risk-Based Internal Audit (RBIA) system for all Scheduled Commercial Banks (except Regional Rural Banks) in 2002. In 2021, it has been decided to mandate RBIA framework for the Non-Banking Financial Companies (NBFCs) and Primary (Urban) Co-operative Banks (UCBs). In Risk Based Internal Audit, role of internal auditor is not only to mitigate current risk, but also to identify new risk areas and mitigate and protect financial system from these risks.

I congratulate CA. Prakash Sharma, Chairman and CA. Priti Paras Savla, Vice-Chairperson and other members of Board of Internal Audit and Management Accounting of ICAI for issuing this "Technical Guide on Risk Based Internal Audit of Non-Banking Financial Company (NBFC)". The Technical Guide is quite comprehensive in its coverage with the objective of augmenting skills and competencies of internal auditors while conducting the risk based internal audit of NBFCs.

I am sure that this Technical Guide will assist the members and others in efficiently discharging their responsibilities.

28th May, 2024
New Delhi

CA. Ranjeet Kumar Agarwal
President, ICAI

Preface

Scheduled Commercial Banks (SCBs) implemented the Risk-Based Internal Audit (RBIA) system in 2002. In 2021, this system was extended to Primary (Urban) Cooperative Banks (UCBs) and Non-Banking Financial Companies (NBFCs) by Reserve Bank of India. A well-defined internal audit policy, functional independence with proper standing, effective communication channels, and sufficient resources for auditing with qualified professionals are the main requirements for this structure. Risk identification, Risk areas prioritisation as audit units and resource allocation accordingly are main requirements of risk-based internal audit.

The Board of Internal Audit and Management Accounting is issuing "Technical Guide on Risk Based Internal Audit of Non-Banking Financial Company (NBFC). This publication gives a basic understanding about NBFCs, legal and regulatory framework thereof, key products, regulators initiatives and future outlook. This publication gives an overview of Risks Faced by NBFCs. It gives a brief overview of steps to be undertaken in Risk-Based Internal Audit in Banks in critical areas such as Sales and Marketing, Know your Customer, Credit Underwriting, Credit Risk management, Loan Books Assets Liability Management, Liquidity Management, Securitization, Outsourcing Management, Customer Services, Finance and Accounts, Information Security. This Guide also explains factors that would be considered while conducting internal audits like functional independence, communication channels and performance evaluation, professional qualifications.

We are immensely grateful to CA. Deepti Rathor and CA. Bharat Ramani for sharing their experience and knowledge with us and preparing the draft of the Guide.

We would like to give special appreciation to CA. Ranjeet Kumar Agarwal, President, ICAI and CA. Charanjot Singh Nanda, Vice-President, ICAI for their continuous support and encouragement to the initiatives of the Board. We are extremely thankful to CA. Rajendra Kumar P, Chairman, BIA&MA (2023-24) who has been the guiding force behind the issuance of this publication. We must also thank our colleagues from the Council at the Board, viz. CA. (Dr.) Rajkumar Satyanarayan Adukia, CA. Chandrashekhar Vasant Chitale, CA. Piyush Sohanrajji Chhajed, CA. Vishal Doshi, CA. Durgesh Kumar Kabra, CA. Sridhar Muppala, CA. Prasanna Kumar D,

CA. Cotha S Srinivas, CA. (Dr.) Debashis Mitra, CA. (Dr.) Rohit Ruwatia Agarwal, CA. (Dr.) Anuj Goyal, CA. Gyan Chandra Misra, CA. Sanjay Kumar Agarwal, CA. Pramod Jain, CA. (Dr.) Sanjeev Kumar Singhal, Shri Deepak Kapoor and Shri Chandra Wadhwa who have always been a significant part of all our endeavours.

We also wish to express our sincere appreciation for CA. Arti Bansal, Secretary, Board of Internal Audit and Management Accounting, ICAI, Mr. Harish Dua, Advisor, and her team for their efforts in giving final shape to the publication.

We firmly believe that this publication would serve as basic guide for the members and other readers interested in the subject.

We will be glad to receive your valuable feedback at biama@icai.in. We also request you to visit our website https://internalaudit.icai.org/ and share your suggestions and inputs, if any, on internal audit.

CA. Prakash Sharma
Chairman
Board of Internal Audit &
Management Accounting

CA. Priti Paras Savla
Vice-Chairperson
Board of Internal Audit &
Management Accounting

Contents

Chapter 1
Introduction

1.1 Non-Banking Financial Companies (NBFCs) have a long history in India spanning several decades and has witnessed significant evolution over time. This concept started way back in 1960's to serve the need of the savers and investors whose financial requirements were not sufficiently covered by the existing banking system. It started with deposit taking NBFCs but did not make big impact initially as the people were not convinced with a company other than a Bank to provide them with financial security.

Asset Finance Companies were introduced in 1997, which primarily focused on providing finance for the acquisition of physical assets like vehicles, machinery, and equipment.

However, during this time, the Indian financial sector faced a crisis due to the failure of several NBFCs.

A new category – Core Investment Companies (CIC) was introduced in year 2006 - engaged in the business of acquisition of shares and securities.

In 2016 another new category – Infrastructure Finance companies (IFC) was introduced to promote investment in infrastructure projects.

Today, NBFCs have diversified into various segments including asset financing, infrastructure financing, microfinance, housing finance, Gold Loans and more. They have evolved substantially in terms of operations, variety of market products and instruments, technological sophistication, etc. They play a crucial role in providing financial services to underserved segments of the population, supporting economic growth, and contribute significantly to the country's financial inclusion efforts.

The future of NBFCs in India is likely to be shaped by digital transformation, regulatory changes, risk management, and customer-centric innovations. NBFCs that can adapt to these changes, maintain strong governance, effectively manage risks will continue to thrive and contribute significantly to India's financial landscape and economic development.

Objective and Scope of Technical Guide

1.2 With financial sector growth, more inclusion expected, and variety of

lending solutions are being launched, it becomes imperative that both Banks and in particular NBFCs sector in India, introduce robust systems and processes that not only address the problems related to internal control and financial transparency but also bring effective governance so as to serve the interests of the various stakeholders and the society, at large.

This Technical Guide disseminates knowledge on Risk Based Internal Audit (RBIA) of NBFCs.

An independent and effective internal audit function in a financial entity provides vital assurance to the Board and its senior management regarding the quality and effectiveness of the entity's internal control, risk management and governance framework. The essential requirements for a robust internal audit function include sufficient authority, proper stature, independence, adequate resources and professional competence.

The internal audit function should broadly assess and contribute to the overall improvement of the organization's governance, risk management, and control processes using a systematic and disciplined approach. This function is an integral part of sound corporate governance and is considered as the third line of defence.

This Technical Guide has been prepared with the objective of augmenting skills and competencies of internal auditors to conduct risk based internal audit of NBFCs.

This Technical Guide covers various types of Non-Banking Financial Companies. The key objective of this guide is to empower internal auditors with practical insights systematically aligned with RBI Mandates.

The guide is applicable to all types of Non-Banking Financial Companies. The purpose of this guide is to provide practical guidance to the internal auditors primarily related to RBI requirements and to promote good practice in applying Standards on Internal Audit while auditing the NBFCs. However, this Guide is not intended to be an exhaustive listing all the procedures and practices to be followed while conducting an internal audit. The internal auditor is expected to apply his best professional judgement in how to apply the most appropriate audit procedures under the circumstances and as per requirements of the situation.

Non-Banking Financial Company (NBFC)

1.3 A Non-Banking Financial Company (NBFC) is a company registered under the Companies Act, 1956 or under the Companies Act, 2013 engaged

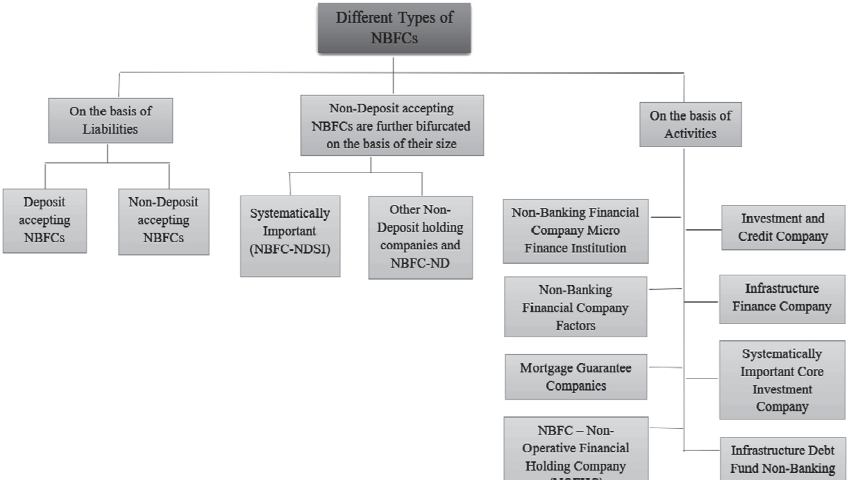
in the business of loans and advances, acquisition of shares/stock/bonds/ debentures/securities issued by the Government or Local Authority or other marketable securities of like nature, leasing, hire-purchase, insurance business, chit business but does not include any institution whose principal business is that of agriculture activity, industrial activity, purchase or sale od any goods (other than securities) or providing any services and sale/ purchase/ construction of immovable property. .

Section 45-I(f) of RBI Act, 1934 defines non-banking financial company as:

(i) a financial institution which is a company;

(ii) a non-banking institution which is a company and which has as its principal business the receiving of deposits, under any scheme or arrangement or in any other manner, or lending in any manner;

(iii) such other non-banking institution or class of such institutions, as the Bank may, with the previous approval of the Central Government and by notification in the Official Gazette, specify.



NBFCs are categorized either in terms of the type of liabilities or in terms of their activities, while Non-Deposit accepting NBFCs are further bifurcated in terms of their size:

(i) Deposit Accepting

Deposit-accepting Non-Banking Financial Companies (NBFCs) are a category of financial institutions in India that are authorized to accept deposits from the public. These NBFCs, unlike other non-deposit accepting NBFCs, have the privilege of mobilizing funds from the public, similar to

banks and provide a wide range of financial services.

Deposit-accepting NBFCs are:

- Allowed to accept and hold deposits from individuals, trusts, companies, and other entities.
- Regulated by the Reserve Bank of India (RBI) and must obtain a Certificate of Registration (CoR) from the RBI to operate as a deposit-accepting NBFC.
- Required to maintain a minimum level of net-owned funds (NOF) as prescribed by the RBI.
- Must follow regulations on capital adequacy, liquidity management, and asset quality.

(ii) Non-Deposit Accepting

Non-deposit accepting NBFCs are further defined by their size into systemically important and other non-deposit holding companies.

A non-deposit accepting Non-Banking Financial Company (NBFC) is a type of financial institution in India that operates as an NBFC but does not have the authorization to accept public deposits. These NBFCs primarily engage in lending and investment activities, providing various financial services to individuals and businesses.

They rely on other sources of funding, such as, borrowing from banks, financial institutions, issuing debentures, and equity capital, to finance their operations.

They are required to manage their assets and liabilities prudently. They must adhere to asset classification, income recognition, and provisioning norms set by the RBI.

(iii) Various Types of NBFCs

Within this broad categorization, RBI has categorized NBFCs as:

- **Asset Finance Company (AFC)**: An AFC is a company which is a financial institution carrying on as its principal business the financing of physical assets supporting productive/economic activity, such as automobiles, tractors, lathe machines, generator sets, earth moving and material handling equipment, moving on own power and general-purpose industrial machines. Principal business for this purpose is

defined as aggregate of financing real/physical assets supporting economic activity and income arising therefrom is not less than 60% of its total assets and total income respectively.

- **Investment Company (IC)**: IC means any company which is a financial institution carrying on as its principal business the acquisition of securities,
- **Loan Company (LC)**: LC means any company which is a financial institution carrying on as its principal business the providing of finance whether by making loans or advances or otherwise for any activity other than its own but does not include an Asset Finance Company.
- **Infrastructure Finance Company (IFC)**: IFC is a non-banking finance company a) which deploys at least 75 per cent of its total assets in infrastructure loans, b) has a minimum Net Owned Funds of ₹ 300 crore, c) has a minimum credit rating of 'A 'or equivalent d) and a CRAR of 15%.
- **Systemically Important Core Investment Company (CIC-ND-SI)**: CIC-ND-SI is an NBFC carrying on the business of acquisition of shares and securities which satisfies the following conditions:
    - It holds not less than 90% of its Total Assets in the form of investment in equity shares, preference shares, debt or loans in group companies.
    - Its investments in the equity shares (including instruments compulsorily convertible into equity shares within a period not exceeding 10 years from the date of issue) in group companies constitutes not less than 60% of its Total Assets.
    - It does not trade in its investments in shares, debt, or loans in group companies except through block sale for the purpose of dilution or disinvestment.
    - It does not carry on any other financial activity referred to in Section 45I(c) and 45I(f) of the RBI act, 1934 except investment in bank deposits, money market instruments, government securities, loans to and investments in debt issuances of group companies or guarantees issued on behalf of group companies.
    - Its asset size is ₹ 100 crore or above and
    - It accepts public funds.

- **Infrastructure Debt Fund: Non- Banking Financial Company (IDF-NBFC)**: IDF-NBFC is a company registered as NBFC to facilitate the flow of long-term debt into infrastructure projects. IDF-NBFC raise resources through issue of Rupee or Dollar denominated bonds of minimum 5-year maturity. Only Infrastructure Finance Companies (IFC) can sponsor IDF-NBFCs.
- **Non-Banking Financial Company - Micro Finance Institution (NBFC-MFI)**: NBFC-MFI is a non-deposit taking NBFC having not less than 85% of its assets in the nature of qualifying assets which satisfy the following criteria:
    - Loan disbursed by an NBFC-MFI to a borrower with a rural household annual income not exceeding ₹ 1,00,000 or urban and semi-urban household income not exceeding ₹ 1,60,000.
    - Loan amount does not exceed ₹ 50,000 in the first cycle and ₹ 1,00,000 in subsequent cycles.
    - Total indebtedness of the borrower does not exceed ₹ 1,00,000.
    - Tenure of the loan not to be less than 24 months for loan amount in excess of ₹ 15,000 with prepayment without penalty.
    - Loan to be extended without collateral.
    - Aggregate amount of loans, given for income generation, is not less than 50 per cent of the total loans given by the MFIs.
    - Loan is repayable on weekly, fortnightly, or monthly instalments at the choice of the borrower.
- **Non-Banking Financial Company – Factors (NBFC-Factors):** NBFC-Factor is a non-deposit taking NBFC engaged in the principal business of factoring. The financial assets in the factoring business should constitute at least 50 percent of its total assets and its income derived from factoring business should not be less than 50 percent of its gross income.
- **Mortgage Guarantee Companies (MGC):** MGC are financial institutions for which at least 90% of the business turnover is mortgage guarantee business or at least 90% of the gross income is from mortgage guarantee business and net owned fund is ₹ 100 crore.
- **NBFC- Non-Operative Financial Holding Company (NOFHC):** is financial institution through which promoter / promoter groups will be

permitted to set up a new bank. It's a wholly owned Non-Operative Financial Holding Company (NOFHC) which will hold the bank as well as all other financial services companies regulated by RBI or other financial sector regulators, to the extent permissible under the applicable regulatory prescriptions.

Legal and Regulatory Framework

1.4 Overview of Regulators of Non-Banking Financial Company is as follows:

Overview of Regulators of Non-Banking Companies

Companies (Registered under Section 3 of the Companies Act 1956)

NBFCs registered with RBI*

Regulation, Supervision, Surveillance & Enforcement under RBI

NBFCs regulated by Other Regulators

Types of Financial Institutions	Authority for Regulation, Supervision, Surveillance & Enforcement
Housing Finance Institutions	National Housing Bank
Merchant Banking Company, Venture Capital Fund Companies, Stock Broking, Collective Investments Schemes (CIS)	SEBI
Nidhi Companies, Mutual Benefit Companies	MCA
Chit Fund Companies	State Government
Insurance Companies	IRDA

Non Banking Non Financial Companies

Regulation, Supervision and Surveillance under the Companies Act 1956

Regulator: Ministry of Corporate Affairs (MCA)

Enforcement Agency: State Governments

Source: Reserve Bank of India

Reserve Bank of India (RBI)

Non-Banking Financial Companies are regulated by the Reserve Bank of India. The Reserve Bank regulates and supervises the NBFCs in terms of Chapter III B of the Reserve Bank of India Act, 1934. The Department of Non-Banking Supervision (DNBS) of RBI is entrusted with the responsibility of regulation and supervision of NBFCs under the regulatory provisions contained under Chapter III B and C and Chapter V of the Reserve Bank of India Act, 1934.

The Regulatory and Supervisory Framework of the Reserve Bank provides for, among other things, registration of NBFCs, prudential regulation of

various categories of NBFCs, issue of directions on acceptance of deposits by NBFCs and surveillance of the sector through off-site and on-site supervision. Deposit accepting NBFCs and Systemically Important Non-Deposit Accepting Companies are subjected to a greater degree of regulation and supervision. The focus of regulation and supervision is three-fold, *viz*., a) depositor protection, b) consumer protection and c) financial stability. The RBI has also been empowered under the Reserve Bank of India Act, 1934 to take punitive action which includes cancellation of Certificate of Registration, issue of prohibitor orders from accepting deposits, filing criminal cases or winding up petitions under provisions of Companies Act in extreme cases.

Regulatory Structure for NBFCs

Regulatory structure for NBFCs comprises of four layers based on their size, activity, and perceived riskiness. NBFCs in the lowest layer are known as NBFC - Base Layer (NBFC-BL). NBFCs in middle layer and upper layer are known as NBFC - Middle Layer (NBFC-ML) and NBFC - Upper Layer (NBFC-UL), respectively. The Top Layer is ideally expected to be empty and known as NBFC - Top Layer (NBFC-TL).

All existing types of NBFCs will be defined in terms of following layers:

- **Base Layer:** The Base Layer shall comprise of (a) non-deposit taking NBFCs below the asset size of ₹1000 crore and (b) NBFCs undertaking the following activities- (i) NBFC-Peer to Peer Lending Platform (NBFC-P2P), (ii) NBFC-Account Aggregator (NBFC-AA), (iii) Non-Operative Financial Holding Company (NOFHC) and (iv) NBFCs not availing public funds and not having any customer interface.
- **Middle Layer**: The Middle Layer shall consist of (a) all deposit taking NBFCs (NBFC-Ds), irrespective of asset size, (b) non-deposit taking NBFCs with asset size of ₹1000 crore and above and (c) NBFCs undertaking the following activities (i) Standalone Primary Dealers (SPDs), (ii) Infrastructure Debt Fund - Non-Banking Financial Companies (IDF-NBFCs), (iii) Core Investment Companies (CICs), (iv) Housing Finance Companies (HFCs) and (v) Infrastructure Finance Companies (NBFC-IFCs).
- **Upper Layer**: The Upper Layer shall comprise of those NBFCs which are specifically identified by the Reserve Bank as warranting enhanced regulatory requirement based on a set of parameters and scoring methodology as provided in the circular. The top ten eligible NBFCs in

terms of their asset size shall always reside in the upper layer, irrespective of any other factor.

- **Top Layer**: The Top Layer will ideally remain empty. This layer can get populated if the Reserve Bank is of the opinion that there is a substantial increase in the potential systemic risk from specific NBFCs in the Upper Layer. Such NBFCs shall move to the Top Layer from the Upper Layer.

National Housing Board (NHB)

National Housing Bank (NHB) was set up by an Act of Parliament in 1987. NHB is an apex financial institution for housing. The broad functions of NHB as a part of its objective of building a strong, healthy, cost-effective, and viable Housing Finance System include:

- Supervision and grievance redressal regarding Housing Finance Companies (HFCs).
- Financing
- Promotion and Development.

It is to be noted that NHB supervises HFCs while regulation of HFCs is with RBI.

Securities and Exchange Board of India (SEBI)

NBFCs listed on stock exchange in India are also regulated by SEBI, the regulatory body for securities markets in India. concerning their conduct of business and reporting requirements. This is apart from the usual compliance and reporting requirements of the RBI and Companies Act under which it is incorporated.

The internal auditor should understand the compliance requirements under various enactments which would help the conduct of internal audit. With the business getting complex and globalisation of finance business, the monitoring agencies make amendments to the existing rules and regulations. The auditor should be aware of such amendments affecting the entity being audited.

Companies Act, 2013

NBFCs are also governed by the Companies Act, 2013. Under this act, NBFCs are required to comply with various provisions related to corporate governance, financial reporting, and statutory compliance.

Anti-Money Laundering Laws and Regulations

The Prevention of Money Laundering Act, 2002 (PMLA)

The anti-money laundering laws in India are framed within a comprehensive framework consisting of the Prevention of Money Laundering Act, 2002, its associated rules, and regulations developed by regulatory bodies such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI). Together, these laws and regulations form a robust framework for preventing money laundering activities in the country.

Section 3 of the PML Act deals with the offence of money-laundering. "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering."

Section 4 of the Act provides that Punishment for money-laundering. "Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years, but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees."

The objectives of the Act include:

Preventing and controlling money laundering.

- To seize and confiscate property derived from or involved in money laundering.
- To provide a penalty for the crime of money laundering.
- To appoint an Adjudicating Authority and an Appellate Tribunal to handle money laundering cases.
- To impose record-keeping obligations on banks, financial institutions, and intermediaries.
- To address any other issues related to money laundering in India.

The Benami Transactions (Prohibition) Act, 1988

The term 'benami' transaction is defined by the Act as a transfer of property from one person to another, where the consideration for the transfer is paid by someone else. The Act, which was enacted in 1988, aims to restrict such transactions and empower authorities to reclaim properties held under benami. Section 3 of the Act explicitly prohibits individuals from engaging in

benami transactions. Also, the Act outlines the properties acquired through benami transactions that can be seized by competent authorities without any obligation to provide compensation.

The Foreign Exchange Management Act, 1999 (FEMA)

The Foreign Exchange Management Act (FEMA), 1999 was enacted by the Parliament "to consolidate and amend the law relating to foreign exchange with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of foreign exchange market in India". FEMA was passed on 29 December 1999, which replaced the Foreign Exchange Regulation Act (FERA).

Under this act, if a taxpayer violates the provisions, they will be liable to pay a penalty equal to three times the amount of default, if it can be quantified, or a penalty of Rs. 2 lakhs if the amount cannot be quantified. If the taxpayer continues to commit the offence, the penalty increases to Rs. 5,000 for each day of default. Furthermore, the relevant authority may seize any currency, securities or other assets belonging to the taxpayer on behalf of the Central Government. The officer is also authorized to repatriate the offender's foreign exchange earnings back to India.

The RBI's Know Your Customer (KYC) Master Directions

The RBI, India's central bank, has issued KYC Master Directions that apply to all entities regulated by the RBI, including banking companies and NBFCs. The objective of these directions is to prevent regulated entities from being exploited for money laundering or terrorist financing activities. The RBI KYC Master Directions require regulated entities to establish customer identity, categorize customers based on the risk they pose, undertake client due diligence (CDD) (including enhanced CDD for high-risk customers and beneficiary accounts), establish procedures for handling various types of transactions, such as cross-border transactions, and report such transactions to the Financial Intelligence Unit (FIU).

The SEBI Anti-Money Laundering (AML) Guidelines

SEBI, the regulatory body for securities markets in India, has issued AML Guidelines that apply to intermediaries registered with SEBI. These guidelines mandate that intermediaries establish policies and procedures to prevent money laundering, which must include communication of group policies related to preventing money laundering and terrorist financing to

management and staff who handle account information, securities transactions, client acceptance policies, and CDD measures (including proper identification requirements), maintenance of records, collaboration with law enforcement authorities (including timely information disclosure), and the use of internal audits or compliance functions to ensure adherence to policies, procedures, and controls related to preventing money laundering and terrorist financing.

Chapter 2
Understanding NBFC

Governance, Board of Directors and Committees

Corporate Governance Frameworks

2.1 Corporate Governance refers to a set of system, principles and process by which an organization is governed. It underpins guidelines as to how an organization can be directed to meet its goals such that it adds value and is beneficial for shareholder as well. Since corporate Governance also set up a framework for attaining an organization's objectives, it covers practically every facet of management, from internal controls and action plans to performance measurement & corporate disclosure. A transparent and agile corporate governance empowers a company to make informed and ethical decisions which omit anything which is against the stakeholder's interest.

RBI has issued guidelines RBI/DNBR/2016-17/45 Master Direction DNBR.PD.008/03.10.119/2016-17 to ensure strict vigil and transparency in operations of the NBFC sector considering public interest and to prevent the affairs of any Systemically Important Non-Deposit taking Non-Banking Financial Company (NBFC-ND-SI) and Deposit taking Non-Banking Financial Company (NBFC-D) from being conducted in a manner detrimental to the interest of investors and depositors or in any manner prejudicial to the interest of such NBFC.

Roles and Responsibilities of Senior Management in the Corporate Governance Structure

Board of Directors and Roles and Responsibilities	**Constitution of Committees of the Board:** **(1) Audit Committee** All Applicable NBFCs shall constitute an Audit Committee, consisting of not less than three members of its Board of Directors. The Audit Committee constituted by a non-banking financial company as required under Section 177 of the Companies Act, 2013 shall be the Audit Committee for the purposes and shall

	have the same powers, functions and duties as laid down in Section 177 of the Companies Act, 2013. The Audit Committee must ensure that an Information System Audit of the internal systems and processes is conducted at least once in two years to assess operational risks faced by the NBFCs. **(2) Nomination Committee** All Applicable NBFCs shall form a Nomination Committee to ensure 'fit and proper' status of proposed/ existing directors. The Nomination Committee constituted under this paragraph shall have the same powers, functions and duties as laid down in Section 178 of the Companies Act, 2013. **(3) Risk Management Committee** To manage the integrated risk, all Applicable NBFCs shall form a Risk Management Committee, besides the Asset Liability Management Committee. **Fit and Proper Criteria:** (1) All Applicable NBFCs shall (i) ensure that a policy is put in place with the approval of the Board of Directors to ascertain the fit and proper criteria of the directors at the time of appointment, and on a continuing basis. (ii) obtain a declaration and undertaking from the directors giving additional information on the directors in the prescribed format. (iii) obtain a Deed of Covenant signed by the directors in the prescribed format (iv) furnish to the Reserve Bank a quarterly statement on the change of directors, and a certificate from the Managing Director of the NBFC that fit and proper criteria in selection of the directors has been followed. The statement must reach the Regional Office of the Reserve Bank within 15 days of the close of the respective quarter. The statement submitted by NBFCs for the quarter ending March 31, should be certified by the auditors.

	Provided that the Bank, if it deems fit and in public interest, reserves the right to examine the fit and proper criteria of directors of any non-banking financial company irrespective of the asset size of such non-banking financial company. **Disclosure and transparency:** (1) All Applicable NBFCs shall put up to the Board of Directors, at regular intervals, as may be prescribed by the Board in this regard, the following: i. the progress made in putting in place a progressive risk management system and risk management policy and strategy followed by the NBFC; ii. conformity with corporate governance standards viz., in composition of various committees, their role and functions, periodicity of the meetings and compliance with coverage and review functions, etc. (2) All Applicable NBFCs shall also disclose the following in their Annual Financial Statements, with effect from March 31, 2015: i. registration/ license/ authorization, by whatever name called, obtained from other financial sector regulators; ii. ratings assigned by credit rating agencies and migration of ratings during the year; iii. penalties, if any, levied by any regulator; iv. information namely, area, country of operation and joint venture partners with regard to Joint ventures and overseas subsidiaries and v. Asset-Liability profile, extent of financing of parent company products, NPAs and movement of NPAs, details of all off-balance sheet exposures, structured products issued by them as also securitization/ assignment transactions and other disclosures.
Chief Risk Officer and Roles and	• **Applicability:** The Reserve Bank of India (RBI) made it mandatory for Non-Banking Financial Companies having asset size more than Rs. 5,000 crore

Responsibilities	to appoint Chief Risk Officer (CRO) to ensure **risk management practices.** This step has been taken to inundate the fear of liquidity crisis in the NBFC sector as the **role of NBFCs** is increasing day by day. • **Qualifications and Experience:** The CRO should be a senior official within the NBFC hierarchy and possess adequate professional qualifications and experience in risk management. • **Fixed Tenure:** The CRO is appointed for a fixed tenure, subject to approval by the Board. Any premature transfer or removal of the CRO requires Board approval and must be reported to the Department of Non-Banking Supervision and, if applicable, to stock exchanges. • **Independence of the CRO:** The Board must establish policies to ensure the independence of the CRO. The CRO should have direct reporting lines to the MD & CEO or the Risk Management Committee (RMC) of the Board. If reporting to the MD & CEO, the RMC/Board should meet the CRO without the presence of the MD & CEO on a quarterly basis. The CRO should not have any reporting relationship with the business verticals of the NBFC and should not be given any business targets. Additionally, the CRO should not be assigned any other responsibilities ('dual hatting'). • **Role of the CRO:** The CRO should be involved in the identification, measurement, and mitigation of risks. They should review all credit products (retail or wholesale) for inherent and control risks. While the CRO can advise on credit proposals, their role in decision-making should be limited. • **Committee Approach in Credit Sanction Process:** If the NBFC follows a committee approach in the credit sanction process for high-value proposals, and the CRO is a decision-maker, the CRO should have voting power. All committee members involved in the credit sanction process are individually and collectively liable for all aspects, including risk perspectives related to the credit proposal.

Chief Information Security Officer (CISO) and Roles and Responsibilities	• **Need for CISO:** An Information Security Committee (ISC), under the oversight of the Risk Management Committee (RMC) of the Board, shall be formed for managing information security. The constitution of the ISC shall include Chief Information Security Officer (CISO), other representatives from business, IT functions, etc. • **Applicability:** Non-Banking Financial Companies in Top, Upper and Middle Layers need to comply with the Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dt. October 20, 2022 (DoS.CO.CSITEG/SEC.xx/31.01.015/2022-23) • **Qualifications and Experience:** A sufficiently senior level executive shall be designated as the Chief Information Security Officer (CISO). The CISO shall not have any direct reporting relationship with the Head of IT Operations and shall not be given any business targets. • **Independence of the CISO:** A sufficiently senior level executive shall be designated as the Chief Information Security Officer (CISO). The CISO shall not have any direct reporting relationship with the Head of IT Operations and shall not be given any business targets. • **Role of the CISO:** shall ensure that the roles and responsibilities of the CISO are clearly defined and documented covering, at a minimum, the following points: (i) The CISO shall be responsible for driving and ensuring compliance with the extant regulatory instructions on information/ cyber security. (ii) The CISO shall be responsible for articulating and enforcing the policies that a RE uses to protect its information assets apart from coordinating information/ cyber security related issues/ implementation within the RE as well as with relevant external agencies.

	(iii) The CISO shall be an invitee to the IT Strategy Committee and IT Steering Committee. (iv) The CISO shall ensure that current and emerging cyber threats to the financial sector and the RE's preparedness in these aspects are discussed in ISC and other related Committees. (v) The CISO's Office, in co-ordination with Head of IT Operations (as required), shall manage and monitor Security Operations Centre (SOC) and drive cyber security related projects. (vi) The CISO shall coordinate the activities pertaining to Cyber Security Incident Response Team (CSIRT) within the RE. (vii) The CISO shall develop cyber security KRIs and KPIs. (viii) The CISO shall have a robust working relationship with Chief Risk Officer (CRO) to enable a holistic risk management approach. To this effect, the CRO may be invited to ISC meetings. CISO may be a member of (or invited to) Committees on Operational Risk where IT/ Information Security risk is also discussed. (ix) CISO shall place a separate review of cyber security risks/ arrangements/ preparedness of the RE before the Board/ Board level Committee on a quarterly basis. Need for CISO: An Information Security Committee (ISC), under the oversight of the Risk Management Committee (RMC) of the Board, shall be formed for managing information security. The constitution of the ISC shall include Chief Information Security Officer (CISO), other representatives from business, IT functions, etc.
Appointment of Chief Compliance Officer (CCO) and Roles and Responsibilities	**Need for Risk Management**: As part of the overall structure for Corporate Governance, Compliance Function serves a critical role. Accordingly, certain principles, standards and procedures for Compliance Function in NBFC-Upper Layer and NBFC-Middle Layer, keeping in view the principles of proportionality.

	Applicability: Framework for Compliance Function and Role of Chief Compliance Officer in Non-Banking Financial Companies in Upper Layer and Middle Layer (NBFC-UL & NBFC-ML) was raised vide **Compliance Function and Role of Chief Compliance Officer (CCO) – NBFCs dt. April 11, 2022 (Ref.No. DoS.CO.PPG./SEC.01/11.01.005/2022-23)** **Qualifications and Experience:** The CCO shall have a good understanding of the industry and risk management practices, knowledge of regulations, legal requirements, and have sensitivity to Supervisory expectations. **Fixed Tenure:** The CCO shall be appointed for a minimum fixed tenure of not less than 3 years. However, in exceptional cases, the Board / Board Committee may relax the minimum tenure by one year, provided appropriate succession planning is put in place. **Independence of the CCO:** The CCO and Compliance Function shall have the authority to communicate with any staff member and have access to all records or files that are necessary to enable her / him to carry out entrusted responsibilities in respect of Compliance issues. This authority shall flow from the Compliance Policy of the NBFC. There shall not be any 'dual hating,' i.e., the CCO shall not be given any responsibility which brings elements of conflict of interest, especially any role relating to business. **Role of the CCO:** Play the central role in identifying the level of Compliance risk in the organisation. The Compliance risks in existing / new products and processes shall be analysed and appropriate risk mitigants put in place. The Chief Compliance Officer (CCO) shall be a member of the 'new product' committee/s. All new products shall be subjected to intensive monitoring for at least the first six months of introduction to ensure that the indicative parameters of Compliance risk are adequately monitored. The NBFC shall carry out an annual Compliance risk assessment

	in order to identify and assess major Compliance risks faced by them and prepare a plan to manage the risks.
Internal Auditor (IA) Roles and Responsibilities	**Need for Internal Audit Guideline**: NBFCs have grown in size and become systematically important prevalence of different audit system/ approaches in such entities has created certain inconsistencies, risks and gap. **Applicability:** All deposit taking NBFCs, all non-deposit accepting NBFCs (including Core Investment Companies) with asset size of ₹50 billion and above are required to follow Risk Based Internal Audit approach. **Qualifications and Experience:** The Requisite professional competence, knowledge and experience of each internal auditor is essential for the effectiveness of internal audit function. The areas of knowledge and experience may include banking/financial entity's operations, accounting, information technology, data analytics, forensic investigation, among others. The collective skill levels should be adequate to audit all areas of the Supervisory Entity (SE). **Tenure:** The Head of Internal Audit (HIA) shall be appointed for a reasonably long period, preferably for a minimum of three years. The Board should prescribe a minimum period of service for staff in the internal audit function. The Board may also examine the feasibility of prescribing at least one stint of service in the internal audit function for those staff possessing specialized knowledge useful for the audit function, but who are posted in other areas, to have adequate skills for the staff in the internal audit function. **Independence of the Internal Audit function:** The Head of Internal Audit (HIA) shall be a senior executive with the ability to exercise independent judgement. The HIA and the internal audit functionaries shall have the authority to communicate with any staff member and get access to all records that are necessary to carry out the entrusted responsibilities. The HIA shall directly report to either the ACB/Board/ MD & CEO or to the Whole Time Director (WTD). Should the Board of Directors decide to allow the MD & CEO or a WTD to be the

	'Reporting authority', then the 'Reviewing authority' shall be the ACB/Board and the 'Accepting authority' shall be the Board in matters of performance appraisal of the HIA. Further, in such cases, the ACB/Board shall meet the HIA at least once in a quarter, without the presence of the senior management (including the MD & CEO/WTD). The HIA shall not have any reporting relationship with the business verticals of these SEs and shall not be given any business targets. **Role of the Head of Internal Audit :** The HIA should work based on established policies and procedures as approved by the ACB/ Board. Shall undertake an independent risk assessment for the purpose of formulating a risk-based audit plan. This risk assessment would cover risks at various levels/areas (corporate and branch, the portfolio and individual transactions, etc.) as also the associated processes which includes identification of inherent business risks in various activities undertaken, evaluation of the effectiveness of the control systems for monitoring the inherent risks of the business activities ('Control risk') and drawing-up a risk-matrix for both the factors viz., inherent business risks and control risks. Source: Notification on Risk-Based Internal Audit (RBIA) dt. February 03, 2021 (Ref.No. DoS.CO.PPG./SEC.05/11.01.005/2020-21)
Statutory Auditors and Roles and Responsibilities	**Applicability:** NBFCs including HFCs for Financial Year 2021-22 and onwards should adhere to the **Guidelines for Appointment of Statutory Central Auditors (SCAs)/Statutory Auditors (SAs)** in respect of appointment/reappointment. However, non-deposit taking NBFCs with asset size below ₹1,000 crore have the option to continue with their extant procedure. **Tenure:** In order to protect the independence of the auditors/audit firms, NBFCs will have to appoint the SCAs/SAs for a continuous period of three years, subject to the firms satisfying the eligibility norms each year. NBFCs removing the SCAs/SAs before completion of three years tenure shall inform concerned Senior

	Supervisory Manager (SSM)/Regional Office (RO) at RBI about it, along with reasons/justification for the same, within a month of such a decision being taken. An audit firm would not be eligible for reappointment in the same Entity for six years (two tenures) after completion of full or part of one term of the audit tenure. However, audit firms can continue to undertake statutory audits of other Entities. **Independence of the SCAs/ SAs:** The Audit Committee of the Board (ACB)/ LMC shall monitor and assess the independence of the auditors and conflict of interest position in terms of relevant regulatory provisions, standards and best practices. Any concerns in this regard may be flagged by the ACB/LMC to the Board of Directors of the NBFC and concerned SSM/RO of RBI. In case of any concern with the Management of the NBFCs such as non-availability of information/non-cooperation by the Management, which may hamper the audit process, the SCAs/SAs shall approach the Board/ACB/LMC, under intimation to the concerned SSM/RO of RBI. Concurrent auditors of the NBFC should not be considered for appointment as SCAs/SAs of the same Entity. The audit of the Entity and any entity with large exposure to the Entity for the same reference year should also be explicitly factored in while assessing the independence of the auditor. **Role of the SCAs/ SAs:** The SCAs/SAs shall be strictly guided by the relevant professional standards in discharge of their audit responsibilities with highest diligence. Any serious lapses/negligence in audit responsibilities or conduct issues on part of the SCAs/SAs or any other matter considered as relevant shall be reported to RBI within two months from completion of the annual audit. Such reports should be sent with the approval/recommendation of the Board/ACB/LMC, with the full details of the audit firm. In the event of lapses in carrying out audit assignments

	resulting in misstatement of an Entity's financial statements, and any violations/lapses vis-à-vis the RBI's directions/guidelines regarding the role and responsibilities of the SCAs/SAs in relation to Entities, the SCAs/SAs would be liable to be dealt with suitably under the relevant statutory/regulatory framework. **Source:** Guidelines for Appointment of Statutory Central Auditors (SCAs)/Statutory Auditors (SAs) of Commercial Banks (excluding RRBs), UCBs and NBFCs (including HFCs) dt. April 27, 2021 (Ref.No.DoS.CO.ARG/SEC.01/08.91.001/2021-22)

Challenges and Opportunities

2.2 In the past few years, the financial sector has witnessed a significant transformation, and Non-Banking Financial Companies have played a pivotal role in that shift. NBFCs continued to reap immense success in the financial sector and its contribution has surpassed the contribution by the traditional banks. NBFCs have continued its growth, and its contribution to the Indian GDP has gone past the contribution by banks.

Although one may find that NBFCs have been capturing market shares and have made rapid progress than the banks, but small NBFCs have faced difficulty in establishing themselves due to the presence of a few prominent players in the NBFC market, additionally there are many challenges to operate which are summarized as below.

Major Challenges Faced by NBFCs

Regulatory Compliance	•NBFCs need to adhere to complex and evolving regulatory frameworks, which can be challenging to navigate. Changes in regulations can impact their operations and capital requirements.
Customer Trust	•Building and maintaining customer trust is crucial for attracting deposits and borrowers. Any negative publicity can harm an NBFC's reputation.
Governance and Risk Management	•Effective governance and risk management practices are vital. Inadequate governance can lead to financial scandals and regulatory penalties
Technology Adoption	•Embracing technology and digital transformation is essential for staying competitive, but it requires substantial investments and expertise
Economic Downturns	•Economic cycles can impact the asset quality of NBFCs. During economic downturns, defaults and NPAs tend to rise.
Funding Costs	•Access to low-cost funding is crucial for profitability. NBFCs often have higher borrowing costs compared to banks.
Competition	•The NBFC sector is highly competitive, with both traditional financial institutions and fintech startups entering the market. Maintaining a competitive edge can be challenging.
Asset Quality	•Ensuring the quality of the loan portfolio is essential. NBFCs need effective risk assessment and recovery mechanisms to manage non-performing assets (NPAs).
Credit Risk	•NBFCs primarily deal with lending, and managing credit risk is a significant challenge. Defaults by borrowers can lead to significant losses.
Liquidity Management	•Maintaining adequate liquidity is crucial for NBFCs. Sudden liquidity crises can lead to a loss of confidence among investors and depositors.
Securitization and Funding Constraints	•The securitization market, a key source of funding for NBFCs, can be affected by market conditions and regulatory changes.
Rural and Semi-Urban Reach	•Expanding operations in rural and semi-urban areas presents unique challenges, including inadequate infrastructure and credit assessment difficulties
Access to Funding	•Unlike banks, NBFCs cannot create money through deposits. They rely on borrowing funds from various sources, making them vulnerable to market conditions and credit rating fluctuations.
Cybersecurity	•With the increasing digitalization of financial services, NBFCs face cybersecurity threats that can compromise customer data and operations.
•Capital Investments	•Implementing new technologies requires significant investments, which may strain the financial resources of NBFCs, especially smaller ones.

To address some of these challenges NBFC's have started reimagining their operations by making use of technology to meet their stakeholder and customer demands. NBFCs have started adopting business and operational

models powered by technologies that seamlessly facilitate the design, launch, implementation and execution of tailored products and services.

Investing in new technologies and strategic partnerships with incumbent financial institutions and FinTechs also allows NBFCs to lower their costs when it comes to increasing their customer base, lowering customer acquisition costs, servicing existing customers or de-risking the portfolio while trying to overcome the increasing formal credit penetration in a growing economy.

New-age NBFCs are using technology more than ever and harnessing partnership ecosystems across the value chain of lead generation, customer onboarding, underwriting, credit/loan disbursement and collection. Artificial intelligence (AI), machine learning (ML) and big data have equipped lenders to measure individual customer insights and build alternative credit scoring models. Mobile and smartphone penetration has enabled NBFCs to connect with customers having low incomes, who can use their mobiles devices throughout the lending cycle of application, engagement, e-KYC and e-signature for disbursements. Robotic process automation (RPA) has enabled streamlining of operational workflows, increasing productivity, accuracy and cost savings.

Listed below are some of the areas where technology evolution has taken place:

- **Digital Lending**: Technology has enabled the growth of digital lending platforms, which compete with traditional NBFCs. These platforms use data analytics and AI to assess credit risk and disburse loans quickly.
- **Fintech Collaboration:** It is seen that NBFCs collaborate with fintech start-ups to leverage their innovative solutions for improved customer experience, risk assessment, and operations.
- **Payment Innovations:** Digital payment methods, such as UPI (Unified Payments Interface), have disrupted traditional payment systems. NBFCs have started adapting to these changes so that they can offer seamless payment solutions to customers.
- **Data Analytics**: Advanced data analytics tools help NBFCs in credit scoring, customer profiling, and fraud detection. However, managing and securing vast amounts of customer data is a challenge.
- **Regtech:** Regulatory technology solutions assist NBFCs in complying with complex regulatory requirements efficiently.

- **Artificial Intelligence (AI) and Machine Learning (ML)**: AI and ML algorithms are used for risk modelling, customer service chatbots, and automating various processes, reducing operational costs.
- **Mobile Apps:** Mobile apps have become a primary interface for customer interactions. Providing a user-friendly, secure, and feature-rich app is essential.
- **Open Banking**: Open Banking initiatives enable NBFCs to access customer financial data from banks with consent, leading to more personalized services.

Committees of the Board

2.3 There are various committees established by the board of directors and senior management to assist the management in the oversight of the NBFC company's operations. These committees are responsible for specific functions and play a crucial role in ensuring compliance, risk management, and strategic decision-making. The specific committees in an NBFC may vary based on the company's size, complexity, and regulatory requirements. Some important ones are:

Audit Committee

Audit committee is responsible for overseeing the financial reporting process, internal controls, and the audit of the company's financial statements. It ensures that financial information is accurate and reliable. This committee is made of primarily independent directors along with executive directors of the company.

Major responsibility of the Audit committee is to:

- Provide oversight on financial reporting process and disclosure of financial information of the Company to ensure that the financial statement is correct, sufficient, and credible.
- Recommend the appointment, removal, remuneration and terms of appointment of Statutory Auditors and Internal Auditors of the Company.
- Provide approval of payment to Statutory Auditors for any other services rendered by them.
- Review with the management, the Annual Financial Statements and Auditor's Report thereon before submission to the Board for approval with reference to:

- Matters required to be included in the director's responsibility statement to be included in the Board's Report in terms of clause (c) of sub-section (3) of Section 134 of the Companies Act, 2013.
    - Changes, if any, in accounting policies and practices and reasons for the same.
    - Major accounting entries involving estimates based on the exercise of judgment by management.
    - Significant adjustments made in the financial statements arising out of audit findings.
    - Compliance with listing and other legal requirements relating to financial statements.
    - Disclosure of any related party transactions.
    - Modified opinion (s) in the draft audit report
- Review with the management, the quarterly financial statements before submission to the board for approval.
- Review with the management, the statement of uses / application of funds raised through an issue (public issue, rights issue, preferential issue, private placement etc.), the statement of funds utilized for purposes other than those stated in the offer document / prospectus / notice and the report submitted by the monitoring agency monitoring the utilisation of proceeds of a public or rights issue or preferential issue or qualified institutional placement, and making appropriate recommendations to the board to take up steps in this matter;
- Provide approval for transactions of the company with related parties.
- Provide approval for inter-corporate loans and investments.
- Provide oversight on valuation of undertakings or assets of the company, wherever it is necessary.
- Evaluate internal financial controls and risk management systems.
- Review, with management, performance of Statutory and Internal Auditors & adequacy of the internal control systems.
- Review the adequacy of Internal Audit function, if any, including the structure of the internal audit department, staffing and seniority of the official heading the department, reporting structure coverage and frequency of internal audit.

- Discuss with Internal Auditors of any significant findings and follow up there on.
- Review the findings of any internal investigations by the Internal Auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of a material nature and reporting the matter to the Board.
- Discuss with Statutory Auditors before the audit commences, about the nature and scope of audit as well as post-audit discussion to ascertain any area of concern.
- Look into the reasons for substantial defaults in the payment to the depositors, debenture holders, shareholders (in case of non-payment of declared dividends) and creditors, if any.
- Review the functioning of the whistle blower/vigil mechanism.
- Provide approval for appointment of chief financial officer after assessing the qualifications, experience, and background, etc. of the candidate.
- Review Management letters / letters of internal control weaknesses issued by the Statutory Auditors as well as Internal Audit reports relating to internal control weaknesses.
- Oversee implementation of regulatory policies including Anti Money Laundering and KYC (Know your customer) Policies.
- Ensure that an Information System Audit of the internal systems and processes is conducted at least once in two years to assess operational risks faced by the NBFCs.
- Investigate into any matter in relation to the items specified in the relevant section of The Companies Act, 2013 or referred to it by the Board.

Risk Management Committee (RMC)

This committee is tasked with identifying, assessing, and managing various types of risks, including credit risk, market risk, liquidity risk, and operational risk. It helps the NBFC maintain a healthy risk profile.

Major responsibility of the Risk Management Committee is to:

- Identify, measure and monitor various risks faced by the Company.
- Formulate a detailed risk management policy which shall include:

- A framework for identification of internal and external risks specifically faced by the Company, including financial, operational, sectoral, sustainability, information, cyber security risks or any other risk as may be determined by the Committee.
- Measure for risk mitigation including systems and processes for internal control of identified risks.
- Business continuity plan.

- Ensure that appropriate methodology, processes, and systems are in place to identify, monitor and evaluate risks associated with the business of the Company including Stress testing in coordination with business departments.
- Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- Periodically review the risk management policy, including by considering the changing industry dynamics and evolving complexity.
- Keep the Board of Directors informed about the nature and content of its discussions, recommendations, and actions to be taken.
- Appointment, removal, and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
- Mitigate various risks associated with functioning of the Company through Integrated Risk Management Systems, Strategies and Mechanisms.
- Deal with issues relating to credit policies and procedure and manage the credit risk, operational risk, management of policies and process.
- Assist in developing the Policies and verifying the Models that are used for risk measurement to have oversight over implementation of risk and related policies.
- Promote an enterprise risk management competence throughout the organisation, including facilitating development of IT-related enterprise risk management expertise.
- Establish a common risk management language that includes measures around likelihood and impact and risk categories.
- Review and approve risk management framework and related policies to ensure that all material risks are appropriately identified, measured,

monitored, and controlled and are commensurate with the Company's size, nature, and complexities.

Asset Liability Management Committee (ALCO)

ALCO is responsible for managing the balance between the company's assets and liabilities. It helps in optimizing the asset portfolio to ensure liquidity and profitability while managing interest rate risk.

Major responsibility of the ALCO is to:

- Review & monitor macro-economic scenario, impact of industry and regulatory changes monitoring the asset liability gap.
- Strategize action to mitigate liquidity and other risks associated with the asset liability gap. Review and suggest corrective actions on liquidity mismatch, negative gaps and interest rate sensitivities. Formulate a contingency funding plan (CFP) for responding to severe disruptions and develop alternate strategies as deemed appropriate, which take into account changes in Interest rate levels and trends, Loan products and related markets and Monetary and fiscal policy.
- Articulate and monitor liquidity risk tolerance that is appropriate for its business strategy and its role in the financial system and verify adherence to various risk parameters and prudential limits.
- Implement liquidity risk management strategy of the Company and review the risk monitoring system.
- Decide the strategy on the source, tenor and mix of assets & liabilities, in line with business plans, considering the future direction of interest rates. Establish a funding strategy that provides effective diversification in the sources and tenor of funding.
- Provide guidance to Business/treasury to review Interest rate environment, on various components of the Interest Rate model, product pricing for advances, prevailing interest rates etc, approve any changes in the interest rate charged to existing and new customers as per the interest rate model policy and reset frequencies basis overall assessment of the liquidity and interest rate risk.
- Consider product pricing for advances, change in PLR, desired maturity profile and mix of the incremental assets and liabilities, prevailing interest rates offered by market for similar services/products, etc.

- Endeavour to develop a process to quantify the liquidity costs, benefits & risk in the internal product pricing.
- Review behavioural assumptions and validate models for study of assets & liabilities in preparation of Liquidity and Interest Rate Sensitivity Statements and ALM analysis.
- Review stress test scenarios including the assumptions and results.
- Formulate and monitor ALM policy/guidelines for the Company.

Nomination and Remuneration Committee (NRC)

This committee is responsible for selecting and nominating candidates for board positions and determining the compensation packages of the company's executives, including the CEO and other top management.

Major responsibility of the NRC is to:

- Formulate criteria for determining qualifications, positive attributes and independence of a director and recommend to the Board of Directors a policy relating to, the remuneration of the Directors, Key Managerial Personnel and other employees.
- Annually review the structure, size and composition (including the skills, knowledge, experience and diversity) of the Board and make recommendations to the Board with regard to any changes.
- Formulate criteria for evaluation of performance of independent directors and the Board of Directors and whether to extend or continue the term of appointment of the independent director, on the basis of the report of performance evaluation of independent director.
- Specify manner for effective evaluation of performance of the Board, its committees and individual Directors and review its implementation and Compliance.
- Identify the persons who are qualified to become directors and who may be appointed in senior management in accordance with the criteria laid down, explore their interest and availability for board / senior management service, recommend to the Board their appointment and removal as and when need arise.
- To ensure ‘fit and proper’ status and credentials of proposed /existing Directors.

- Annually review and recommend the salary, bonus, equity option plan other compensation to the Key Employees as well as the quantitative & qualitative objectives for the relevant Financial Year and the Key Performance Indicators (KPI) structure associated with the award of any incentives.
- Make recommendations to the Board regarding policy relating to the remuneration for the Directors, Key Employees and other employees and plans for succession for both executive and non-executive Directors, Key Employees as well as Senior Management
- Review the performance of Key Employees in case of significant underperformance by the Company with respect to expected profitability, net worth, quality of assets, etc. and review the reasons for such under performance and evaluate the performance of Key Employees.

IT Strategy Committee

In today's digital age, technology plays a critical role in the operations of NBFCs. This committee focuses on technology-related strategies, cybersecurity, and innovation initiatives.

Major responsibility of the IT Strategy Committee is to:

- Approve IT strategy and policy documents, within the framework approved by the Board, and ensuring that the management has put an effective strategic planning process in place.
- Ascertain that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensure IT investments represent a balance of risks and benefits and that budgets are acceptable.
- Monitor the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.
- Ensuring proper balance of IT investments for sustaining company’s growth and becoming aware about exposure towards IT risks and controls.
- Institute an appropriate governance mechanism for outsourced processes, comprising of risk-based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end-to-end manner.

- Develop sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements.

Credit Committee

In NBFCs involved in lending activities, the credit committee is responsible for approving loans and setting credit policies and guidelines. It ensures that lending decisions align with the company's risk appetite and credit standards.

Major responsibility of the Credit Committee is to:

- Approve all lending transactions in accordance with the defined Delegation of Power matrix as stipulated from time to time.
- Approve credit/lending limits and deviation matrix and regulatory limits as prescribed from time to time.
- Approve purchase, sale, transfer of financial assets to/from Asset Reconstruction Company, Securitization Company, other Non-Banking Financial Companies, Banks, Financial Institutions, etc.
- Review the Investment Policy for the Company.
- Invest/ disinvest the funds of the Company under various financial products, for such period and on such terms and conditions, as they may deem fit and proper, within the limits as set out by the Board.

Know Your Customer (KYC) Procedures Including Customer Due Diligence

2.4 In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

In terms of the provisions of Prevention of Money Laundering Act, 2002 (PML Act) and the Prevention of Money Laundering (Maintenance of records) Rules, 2005 (PML Rules), reporting entities (RE) are required to follow Customer Identification Procedures (CIP) while undertaking a transaction at the time of establishing an account-based relationship/ client-based relationship and monitor their transactions on-going basis. In this respect, the RBI introduced norms for KYC and AML to be followed by the NBFCs in carrying out business transactions of accepting deposits and lending to customers. The master direction on KYC provides a comprehensive framework that seeks to promote transparency, accountability, and customer protection in the financial system.

NBFCs are required to frame KYC policy duly approved by the Board of Directors of NBFC or any committee of the Board to which power has been delegated comprising of four key elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures (CIP); and

(d) Monitoring of Transactions.

NBFC need to ensure that the KYC norms/ AML standards/ CFT measures have been prescribed in the policy and that they ensure that criminals are not allowed to misuse the banking/ financial channels. It would, therefore, be necessary that adequate screening mechanism is put in place by NBFCs as an integral part of their recruitment/ hiring process of personnel.

Asset Liability Management (ALM)

2.5 Asset and Liability Management (ALM) in a Non-Banking Financial Company (NBFC) is a critical function that involves managing the company's assets and liabilities to ensure the stability and profitability of the organization. ALM aims to strike a balance between the assets (loans, investments, etc.) and liabilities (borrowings, deposits, etc.) of an NBFC taking into consideration various factors like interest rate risk, liquidity risk, and profitability. etc.

Asset and Liability Management is the set of actions and procedures designed to control risks and financial position. Safety and soundness issues are an important part of this definition.

The assets and liabilities must be managed to achieve satisfactory and consistent earnings, liquidity, and safety. The Company should believe in not relying on interest rates and other factors and therefore, establish policies and procedures for Asset Liability management to appropriately manage the risks and financial position. The Company should also recognize the importance of liquidity/funds management in effectively managing its balance sheet and related earnings stream.

The characteristics of Assets and Liabilities management in an NBFC:

- Overcome the asset-liability mismatches, interest risk exposures, etc.
- Ensure overall system for effective risk management.
- Measure and manage the various Risks facing the company on a consistent basis.
- Establish guidelines to meet various applicable regulatory rules and statutes.
- Form a consistent co-policy with other policies (investments, lending, operations, etc.)
- Coordinate the management of the company’s financial position and
- Maintain a good balance among spreads, profitability and long-term viability.

Reserve Bank of India (RBI) vide its Circular No. DNBS (PD).CC.No.15 /02.01 / 2000-2001 dated June 27, 2001 prescribed Guidelines for Asset-Liability Management and has mandated all NBFCs with asset size exceeding ₹ 100 crores to put in place an ALM system. The guidelines also prescribe for making and submission of periodic reporting to RBI.

RBI vide its Circular No. DOR.NBFC(PD) CC.No.102/03.10.001/2019-20 dated November 4, 2019 released further guidelines on Liquidity Risk Management Framework for all non-deposit taking NBFCs with asset size of 100 Cr and above. The guidelines recast some existing regulatory prescriptions on ALM framework and introduced certain other features including disclosure standards.

Responsibility

Board of Directors: The Asset Liability management policy should fall under the authority of the Board of Directors, who in turn can assign the authority for its administration and revision to the Assets and Liabilities Committee. The ultimate responsibility for effective Asset Liability management would rest with the Board of Directors of the Company. It should also decide the risk management policy of the Company and set limits for liquidity, interest rate and securities price risk. It is the responsibility of the Board that guidelines under Liquidity Risk Management framework are adhered to. The Board shall decide the strategy, policies and procedures to manage liquidity risk.

The Asset Liability Management Committee (ALCO): ALCO should be constituted and the broad objectives of forming the ALCO should be:

Liquidity Risk

The role of the ALCO with respect to liquidity risk would include, inter alia, decision on desired maturity profile and mix of incremental assets and liabilities, sale of assets as a source of funding, the structure, responsibilities and controls for managing liquidity risk, and overseeing the liquidity positions across the organisation etc.

Liquidity Management

To monitor the asset liability gap and strategize action to mitigate the risk associated.

Ensuring availability of adequate liquid resources with a view to keep

maturity mismatches in the Balance Sheet of the Company within desired levels; and

Interest Rate Risk Management

Reviewing Interest Rates Scenario and decide on the desired composition of various portfolios.

Capture the sensitivity of Market Value of its Equity (MVE) to interest rate movements.

Profit Planning

Positioning in order to maximize shareholder value while protecting the company from any adverse consequences arising from liquidity and interest rate risk.

Asset and Liability Management in an NBFC involves a comprehensive approach to managing the company's financial resources to optimize profitability while minimizing risks. Effective ALM helps NBFCs maintain financial stability, adapt to changing market conditions, and comply with regulatory requirements.

Internal Capital Adequacy Assessment Process (ICAAP)

2.6 RBI has issued “Scale Based Regulation (SBR)” for the NBFC sector in India vide their circular RBI/2021-22/112 DOR.CRE.REC. No.60/03.10.001/2021-22 dated 22 October 2021 which is effective from 01 October 2022.

Accordingly, NBFC’s are categorized in four layers –Base Layer (NBFC-BL), Middle Layer (NBFC-ML), Upper Layer (NBFC-UL) and Top Layer (NBFC-TL). Categorization is done based on their size, activity, and perceived riskiness. The Top Layer is ideally expected to be empty unless Reserve Bank is of the opinion that there is a substantial increase in the potential systemic risk from specific NBFCs in the Upper Layer and those will then be moved to Top Layer.

The top ten eligible NBFCs in terms of their asset size shall always reside in the upper layer, irrespective of any other factor (currently there are 15 NBFCs in upper layer). Also, NBFC-D, CIC, IFC and HFC will be included in Middle Layer or the Upper Layer (and not in the Base layer), as the case may be. SPD and IDF-NBFC will always remain in the Middle Layer.

Under the Regulatory changes stated by RBI under the SBR applicable to NBFC-ML and NBFC-UL, NBFCs are required to have an ICAAP (Internal Capital Adequacy Assessment Policy) in place. NBFCs are required to make a thorough internal assessment of the need for capital, commensurate with the risks in their business. The methodology for internal assessment of capital shall be proportionate to the scale and complexity of operations as per their Board approved policy. The objective of ICAAP is to ensure availability of adequate capital to support all risks in business as also to encourage NBFCs to develop and use better internal risk management techniques for monitoring and managing their risks. The circular also suggests that the internal assessment shall be on similar lines as ICAAP prescribed for commercial banks under Pillar 2 (Master Circular – Basel III Capital Regulations dated July 01, 2015).

ICAAP Principles

The ICAAP is an important component of Pillar 2 i.e., Supervisory Review and Evaluation Process (SREP) requirements for Basel III regulations.

It envisages the establishment of suitable risk management system in the Company and their review by supervisory authority.

Under Pillar 2, the Company shall implement the process for assessing their capital adequacy in relation to their risk profiles as well as a strategy for maintaining their capital levels – i.e., Internal Capital Adequacy Assessment Process (ICAAP) in addition to the capital specified under Pillar 1 of Basel Accord

Based on the referred RBI regulations, the main aspects to be addressed under the SREP, and therefore, under the ICAAP, includes:

- The risks that are not fully captured by the minimum capital ratio prescribed under Pillar 1
- The risks that are not at all considered by the Pillar 1; and the factors external to the Company.
- The organization should follow below key principles while implementing ICAAP:

Active Board and Senior Management Oversight

The process should be supported by Board and Senior Management's oversight, sound capital management, comprehensive assessment of risks, monitoring and reporting and internal control review.

Appropriate Policies, Procedures and Limits

Organization's policies and procedures should provide specific guidance for the implementation of broad business strategies and to establish, where appropriate, internal limits for the various types of risk to it may be exposed.

Comprehensive Assessment of Risks

Risk measurement systems should be sufficiently comprehensive and rigorous to capture the nature and magnitude of risks faced by the organization. It should consider strengthening its risk management systems, applying internal limits, increasing the level of provisions and reserves, and improving internal controls. However, the capital should not be considered as a substitute for mitigating fundamentally inadequate control or risk management process.

Identification, Measurement, Mitigation, Controlling, Monitoring and Reporting of Risks

Organization should establish an adequate system for identifying, measuring, monitoring, and reporting risk exposures and assessing how the NBFC's changing risk profile affects the need for capital.

Sound Capital Assessment

NBFC should implement a process for assessing capital adequacy in relation to its risk profile as well as a strategy for maintaining adequate capital levels, known as ICAAP.

Internal Controls Review

NBFC should conduct periodic review of its risk management process to ensure its integrity, accuracy, and reasonableness through internal or external audits. The review should be conducted at least annually or sooner, if warranted by changes in the business/ regulatory environment that it operates in. Any non-compliance with the internal policies and/ or minimum capital requirements shall be reported for timely rectification.

Submission of the Outcome of ICAAP to Board

As ICAAP is a dynamic process; a written record on the outcome of ICAAP should be submitted to the Board of Directors of the company annually. The document should detail the risks identified, the way those risks are monitored and managed, the impact of the changing risk profile on the Company's

capital position including details of stress tests/scenario analysis conducted and the resultant capital requirements.

Direct Sales Agents (DSA)/ Recovery Agents

2.7 The role of a Direct Selling Agent (DSA) can be significant in the operations of a Non-Banking Financial Company (NBFC). DSAs play a crucial role in the distribution and sourcing of loans and financial products for NBFCs.

DSAs can extend the geographical reach of an NBFC, allowing it to tap into markets and customer segments that might not be easily accessible through the NBFC's own branches or marketing efforts. This extended reach can significantly enhance the NBFC's business growth.

DSAs are often responsible for customer acquisition and lead generation. They identify potential borrowers, market the NBFC's products, and facilitate the loan application process.

Using DSAs can be a cost-effective distribution channel for NBFCs. Instead of establishing and maintaining a large network of physical branches, NBFCs can leverage the existing infrastructure and expertise of DSAs, which can help reduce operational costs.

NBFCs often appoint recovery agents to manage collection of due / overdue loans. They are authorised by the Company to use various communication channels, including phone calls, emails, and physical visits to the borrower's residence or workplace.

Effective debt recovery helps NBFCs minimize non-performing assets and maintain their liquidity and financial stability. However, it's important for recovery agents to carry out their responsibilities with empathy, professionalism, and compliance with legal and ethical standards to ensure a fair and transparent process for borrowers.

With opportunities come the challenges. As DSA would be considered as outsourced activities, it comes with its own potential risks. NBFC should have proper mechanism to ensure that:

- All DSA / Recovery Agents shall be properly trained to handle their responsibilities with care and sensitivity, particularly aspects such as soliciting customers, hours of calling, privacy of customer information and conveying the correct terms and conditions of the products on offer, etc.

- The Company should ensure that there is Board approved Code of conduct for DSA / Recovery Agents and obtain their undertaking to abide by the code.
- In addition, Recovery Agents shall adhere to extant instructions on Fair Practices Code issued by the RBI along with Company's own code for collection of dues and repossession of security. It is essential that the Recovery Agents refrain from action that could damage the integrity and reputation of the Company and that they observe strict customer confidentiality.
- The agents shall not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude the privacy of the debtors' family members, referees, and friends, making threatening and anonymous calls or making false and misleading representations.

Co-lending Model (CLM)

2.8 In 2018, RBI introduced the concept of co-origination of loans by banks and NBFCs for lending to priority sector. The arrangement entailed joint contribution of credit at the facility level by both the lenders as also sharing of risks and rewards.

Based on the feedback received from various stakeholders and to better leverage the respective comparative advantages of the banks and NBFCs in a collaborative effort, in November 2020 RBI introduced Co-lending model. The primary focus of the revised scheme, rechristened as "Co-Lending Model" (CLM), is to improve the flow of credit to the unserved and underserved sector of the economy and make available funds to the ultimate beneficiary at an affordable cost, considering the lower cost of funds from banks and greater reach of the NBFCs.

In terms of the CLM, banks are permitted to co-lend with all registered NBFCs (including HFCs) based on a prior agreement. The co-lending banks will take their share of the individual loans on a back-to-back basis in their books. However, NBFCs shall be required to retain a minimum of 20 per cent share of the individual loans on their books.

Essential Features of CLM

The Master Agreement entered by the banks and NBFCs for implementing the CLM may provide either for the bank to mandatorily take their share of

the individual loans as originated by the NBFC in their books or retain the discretion to reject certain loans subject to its due diligence.

If the Agreement entails a prior, irrevocable commitment on the part of the bank to take into its books its share of the individual loans as originated by the NBFC, the arrangement must comply with the extant guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks issued vide RBI/2014-15/497/DBR.No.BP.BC.76/21.04.158/2014-15 dated March 11, 2015 and updated from time to time. In particular, the partner bank and NBFC shall have to put in place suitable mechanisms for ex-ante due diligence by the bank as the credit sanction process cannot be outsourced under the extant guidelines.

The bank shall also be required to comply with the Master Directions - Know Your Customer (KYC) Direction, 2016, issued vide RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 and updated from time to time, which already permit regulated entities, at their option, to rely on customer due diligence done by a third party, subject to specified conditions.

However, if the bank can exercise its discretion regarding taking into its books the loans originated by NBFC as per the Agreement, the arrangement will be akin to a direct assignment transaction. Accordingly, the taking over bank shall ensure compliance with all the requirements in terms of Guidelines on Transactions Involving Transfer of Assets through Direct Assignment of Cash Flows and the Underlying Securities issued vide RBI/2011-12/540 DBOD.No.BP.BC-103/21.04.177/2011-12 dated May 07, 2012 and RBI//2012-13/170 DNBS. PD. No. 301/3.10.01/2012-13 August 21, 2012 respectively, as updated from time to time, except for Minimum Holding Period (MHP) which shall not be applicable in such transactions undertaken in terms of this CLM.

The MHP exemption shall be available only in cases where the prior agreement between the banks and NBFCs contains a back-to-back basis clause and complies with all other conditions stipulated in the guidelines for direct assignment.

The NBFC shall be the single point of interface for the customers and shall enter into a loan agreement with the borrower, which shall clearly contain the features of the arrangement and the roles and responsibilities of NBFCs and banks.

All the details of the arrangement shall be disclosed to the customers upfront, and their explicit consent shall be taken.

The ultimate borrower may be charged an all-inclusive interest rate as may be agreed upon by both the lenders conforming to the extant guidelines applicable to both.

The extant guidelines relating to customer service and fair practices code and the obligations enjoined upon the banks and NBFCs therein shall be applicable mutatis mutandis in respect of loans given under the arrangement.

The NBFC should be able to generate a single unified statement of the customer, through appropriate information sharing arrangements with the bank.

With regard to grievance redressal, suitable arrangement must be put in place by the co-lenders to resolve any complaint registered by a borrower with the NBFC within 30 days, failing which the borrower would have the option to escalate the same with the concerned Banking Ombudsman/ Ombudsman for NBFCs or the Customer Education and Protection Cell (CEPC) in RBI.

The co-lending banks and NBFCs shall maintain each individual borrower's account for their respective exposures. However, all transactions (disbursements/ repayments) between the banks and NBFCs relating to CLM shall be routed through an escrow account maintained with the banks, to avoid inter-mingling of funds. The Master Agreement shall clearly specify the manner of appropriation between the co-lenders.

The Master Agreement may contain necessary clauses on representations and warranties which the originating NBFC shall be liable for in respect of the share of the loans taken into its books by the bank.

The co-lenders shall establish a framework for monitoring and recovery of the loan, as mutually agreed upon.

The co-lenders shall arrange for creation of security and charge as per mutually agreeable terms.

Each lender shall adhere to the asset classification and provisioning requirement, as per the respective regulatory guidelines applicable to each of them including reporting to Credit Information Companies, under the applicable regulations for its share of the loan account.

The loans under the CLM shall be included in the scope of internal/statutory audit within the banks and NBFCs to ensure adherence to their respective

internal guidelines, terms of the agreement and extant regulatory requirements.

Any assignment of a loan by a co-lender to a third party can be done only with the consent of the other lender.

Both the banks and the NBFCs shall implement a business continuity plan to ensure uninterrupted service to their borrowers till repayment of the loans under the co-lending agreement, in the event of termination of co-lending arrangement between the co-lenders.

The Co-Lending Model aims to harness the combined strengths of banks and NBFCs to enhance credit flow to priority sectors, including agriculture, MSMEs, and small traders. This collaboration allows banks to meet their priority sector lending targets while leveraging the on-ground presence and domain expertise of NBFCs.

Note that regulatory guidelines can change over time, so it's advisable to refer to the most recent RBI guidelines and circulars for the most up-to-date information on the Co-Lending Model.

Material Outsourcing Activities Including IT Outsourcing

2.9 In NBFCs, activities that are outsources are as follows:

Outsourcing of Financial Services

In order to get access to specialist expertise and to reduce operational costs, Non-Banking Financial Companies (NBFCs) extensively outsource some of their operations. These outsourced activities were hitherto not regulated and hence, exposed the NBFCs as well as their customers to considerable risks, such as strategic risk, reputation risk, compliance risk, operational risk, legal risk etc. Hence, a need was felt to put in place appropriate safeguards for addressing these risks. RBI issued Directions on Managing risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Companies on November 09, 2017 with a view to lay down a framework for outsourcing for NBFCs. The directions are applicable to material outsourcing arrangements and relate to managing risks in the outsourcing of financial services. The directions are not applicable to technology related issues and activities not related to financial services, such as using couriers, housekeeping, security of premises, movement and archiving of records, etc.

Note: Material outsourcing arrangements are those, which if disrupted, have the potential to significantly impact business operations, reputation, profitability, or customer service. Materiality of outsourcing would be based on:

- Level of its importance to the NBFC and significance of the risk
- Potential impact of outsourcing on the NBFC on parameters such as earnings, solvency, liquidity, risk profile
- Likely impact on the NBFC's reputation and brand value
- Cost of outsourcing
- Aggregate exposure to that particular service provider
- Significance of activities outsourced in context of customer service and protection.

If the NBFC uses service organizations to provide core services or activities, such as cash and securities settlement or back-office activities the responsibility for compliance with rules and regulations and sound internal controls remains with those charged with governance and the management of the outsourcing NBFC. The internal auditor should consider legal and regulatory restrictions and obtains an understanding of how the management and those charged with governance monitor that the system of internal control (including internal audit) operates effectively. Standard on Internal Audit (SIA) 530, "Third Party Service Provider" as issued by ICAI gives further guidance on this subject.

IT Outsourcing

The Reserve Bank of India ("RBI") has issued the RBI Master Direction on Outsourcing of Information Technology Services dated April 10, 2023 ("Directions"), that will come into effect on October 1, 2023, in line with its earlier Draft Master Direction on Outsourcing of IT Services, dated June 23, 2022 ("Draft Directions"). The RBI's message to Regulated Entities ("RE") via these Directions is clear – the liability of Regulated Entities ("RE") towards their customers does not get diminished due to such outsourcing arrangements or on account of engaging Third Party Service Providers ("TPSP"), nor does it impede effective supervision by the RBI.

The Directions apply to 'material outsourcing of information (IT) services', defined as services which:

(i) if disrupted/ compromised have the potential to significantly impact the business operations of RE; and

(ii) may have material impact on RE' customers if there is any unauthorised access, loss or theft of customer information.

Key Highlights of Regulated Entities

- Grievance redressal framework: RE must retain the responsibility of customer grievance redressal.
- Governance Framework: RE must put in place a board-approved comprehensive IT outsourcing policy, governing the roles and responsibilities of the board, committees of the board, senior management, IT function, business function, oversight, and assurance functions in respect of outsourcing of IT services.
- Due Diligence: RE must conduct due diligence on TPSPs based on a risk-based approach, taking into consideration various qualitative, quantitative, legal, reputational, and operational factors, along with associated risks.
- Monitor/ Control: RE must conduct periodic audits to assess key factors such as performance of service providers, risk management activities adopted, etc.
- Risk Management Framework: RE must put in place a robust risk management framework, including the identification, measurement, mitigation/ management and reporting of risks.
- Confidentiality and Security: RE must also be responsible for ensuring that customer data with TPSPs are secure and confidential, with access on a need-to-know basis.
- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP): TPSPs must have an established framework for BCP and DRP.
- Outsourcing to Business Group/ Conglomerate: On the condition that a board-approved policy is in place, RE can outsource IT activities to its business group/ conglomerate.
- Cloud Computing Services: Factors RE must take into consideration while adopting cloud computing services from cloud TPSPs are outlined.
- Security Operations Centre ("SOC"): Outsourcing of operations to an SOC may carry certain risks, particularly since the data is not only

stored and processed at an external location, but also managed by a third party.

These Directions are likely to lead to major changes related to outsourcing arrangements between RE and TPSPs. There is specific focus on data privacy and protection, with the inclusion of confidentiality clauses in the outsourcing agreement as well as segregation of customer data into separate pools by TPSPs such that only a lending RE would have access to the borrower's data.

Suggestive parameters for evaluating the capability of service provider:

- Competence, experience
- External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates.
- Ability to effectively service all the customers with confidentiality where a service provider has exposure to multiple banks.
- Undue concentration of outsourcing arrangements with a single service provider.
- Financial soundness and ability to service even under adversity.
- Capability to identify and segregate RE's data..
- Ensuring due diligence by service provider of his employees and sub-contractors.
- Business reputation, culture, compliance, complaints and outstanding or potential litigation Information/cyber security risk assessment.
- Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed, or stored by the service provider.

Fintech

2.10 FinTech which is short for financial technology, is an industry segment consisting of companies that use technology to make financial services efficient. These are usually start-ups founded with the purpose of disrupting incumbent financial systems and corporations that rely traditional way of servicing rather than using the latest technological trends.

- **Reserve Bank of India stated** *"FinTech is broadly used to describe emerging technological innovations in the financial services sector, with ever-increasing reliance on information technology.*
- **The Financial Stability Board or FSB quoted** *"technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services".*

Fintech Working

Fintech provides people and businesses with access to traditional financial services in innovative ways that previously weren't available. For instance, many conventional banks' mobile apps now offer customers on-the-go access to bank services, including the ability to view your balance, transfer funds or deposit a check.

Fintech also automates many services businesses use, such as loan underwriting and real estate appraisals. Artificial intelligence combined with massive troves of consumer data helps fintech businesses understand their customers and powers their marketing campaigns, product development and underwriting.

Understanding of Areas of Fintech Segments in India

Areas	FinTech Segments	Brief Description
A. Credit	01. Peer-to-Peer Lending 02. Crowd Funding 03. Market Place for Loans 04. Online Lenders – on-book lending by NBFCs 05. Credit Scoring Platforms	• All forms of lending market places including Peer-to-Peer lenders and market places that connect borrowers with both, institutional and lenders; includes crowd funding and equity funding platforms • NBFCs that use alternative scoring and digital channels for acquisition
B. Payments	06. Mobile Wallet (M-wallets) and Prepaid Payment Instruments (PPIs)	• Services that enable transfer of funds for various use cases - P2P (Person-to-Person), P2M (Person-to-Merchant), G2P

	07. Merchant Payments and PoS Services 08. International Remittance	(Government-to-Person) etc. • Services targeted at both Payees and Merchants by enabling requisite payment infrastructure through mobile or other technologies
C. Investment Management	09. Robo Advisors 10. Discount Brokers 11. Online Financial Advisors	• Wealth advisory services delivered through technology governed rules and investment strategies
D. Personal Finance Management	12. Tax Filling and Processing 13. Spend Management and Financial Planning 14. Credit Scoring Services	• Tools and services for active management of individual financial profiles (e.g. spend, investments, credit profile, etc.)
E. Bank tech	15. Big Data 16. Customer Onboarding Platforms	• Services that utilize many data points such as financial transactions, spending patterns to build the risk profile of the customer. This provides an alternate to traditional underwriting methods that are unable to serve people with limited credit data. • There is significant value in unstructured data. However, it is difficult to derive value from unstructured data, owing to challenges in analyzing it. A number of new tools are being developed to derive value from large data sets.
F. InsurTech	17. Insurance	• Insurtech refers to technological innovations

	Aggregator	that are created and implemented to improve the efficiency of the insurance industry. Insurtech powers the creation, distribution, and administration of the insurance business

NBFCs and Fintechs

NBFCs are adopting business and operational models powered by technologies that seamlessly facilitate the design, launch, implementation and execution of tailored products and services. Investing in new technologies and strategic partnerships with FinTechs allows NBFCs to lower their costs when it comes to increasing their customer base, lowering customer acquisition costs, servicing existing customers or de-risking the portfolio while trying to overcome the increasing formal credit penetration in a growing economy.

Present-day FinTech companies are efficiently making use of new-age technologies to overcome challenges and build products and services such as last mile reach and delivery, alternative credit models, fraud detection, regulatory compliance, enterprise automation for accounting, treasury and reconciliation, etc, for traditional NBFCs.

To strengthen its position in the ecosystem, the NBFC's have started building partnerships with FinTech companies specialising in new-age technologies such as Artificial Intelligence and alternative credit scoring, etc.

First Loss Default Guarantee (FLDG)

In the past decade, India's FinTech sector has evolved from niche players to integral solution providers, and now stands at the brink of unprecedented growth in technological advancements and financial inclusion. The Reserve Bank of India (RBI's) recent decision to allow Default Loss Guarantee (DLG) arrangements in digital lending has ushered in a new era of possibilities for the country's FinTech sector. These guidelines, which provide clarity on lending arrangements between FinTechs, banks, and Non-Banking Financial Companies (NBFCs), are poised to reshape the landscape of the industry.

The release of the First Loss Default Guarantee (FLDG) guidelines marks a significant milestone for India's FinTechs. It is the first time that the RBI has approved the FLDG program, which enables credit-risk sharing arrangements between FinTechs and regulated lenders like banks and NBFCs. Under the new rules, the RBI gives the green signal to the FLDG scheme, wherein unregulated entities offer guarantees to regulated lenders in the event of borrower defaults.

In this lending arrangement, a percentage of the default loan portfolio of registered entities is guaranteed by FinTechs or Lending Service Providers. FLDGs empower FinTechs to showcase their underwriting capabilities and earn the trust of banks and NBFCs. Previously, FinTechs provided FLDG guarantees of up to 100 per cent to their banking partners, exposing them to high risks and potential losses. In September 2022, the RBI cracked down on such arrangements, restricting FLDGs to only Regulated Entities (REs).

Some of the Key Highlights of the new framework are –

1. A 5 per cent cap on FLDG arrangements, ensuring that the total default guarantee provided by FinTechs does not exceed 5 per cent of the portfolio amount.
2. FLDG arrangements can only be carried out between RBI-regulated entities and Lending Service Provider (LSPs) or between two regulated entities that have entered into an outsourcing agreement.
3. REs is allowed to invoke FLDG within a maximum overdue period of 120 days, highlighting the RBI's commitment to timely default resolution.
4. REs can accept DLGs only if FinTechs provide a hard guarantee in the form of cash deposits, bank guarantees, or fixed deposits maintained with scheduled commercial banks.
5. The RBI instructs LSPs to publish details of the total number of portfolios and respective amounts on which FLDG has been offered on their websites.
6. REs remains responsible for recognizing individual loans in the portfolio as Non-Performing Assets (NPA) and making necessary provisioning, regardless of the FLDG cover at the portfolio level.

Chapter 3
Key Products

Wholesale Lending

3.1 Wholesale lending Non-Banking Financial Companies (NBFCs) are financial institutions that primarily provide financing solutions to businesses, institutions, and other wholesale borrowers. They are critical to the Indian lending ecosystem, especially when banks cannot meet credit demands due to capital constraints.

Wholesale lending NBFCs primarily cater to the needs of corporate clients, large businesses, and institutions. Their main focus is on providing financing solutions for business expansion, working capital, project finance, and other corporate requirements.

These NBFCs typically deal with larger loan amounts compared to retail focused NBFCs. They are equipped to handle substantial credit needs of corporate clients, which may include loans in the millions or even billions of rupees.

They work with a diverse range of clients, including large corporations, infrastructure companies, real estate developers, government entities, and other institutional borrowers. They may also serve as intermediaries in syndicated loans.

These NBFCs offer customized financing solutions tailored to the specific needs of their corporate clients.

Due diligence and risk assessment play a crucial role in wholesale lending. NBFCs conduct comprehensive credit assessments, financial analysis, and risk evaluations to ensure the creditworthiness of their corporate clients.

Wholesale lending NBFCs often require collateral or security to mitigate risk. This can include assets, property, shares, debentures, or other forms of collateral depending on the nature of the loan and the borrower's profile.

Interest rates for wholesale lending are typically negotiated and may vary depending on factors such as creditworthiness, market conditions, and the type of loan. Interest rates for wholesale loans are usually lower than those for retail loans due to the larger transaction sizes.

Loan tenures in wholesale lending can vary widely depending on the purpose of the loan. Short-term working capital loans may have relatively shorter tenures, while project finance or infrastructure loans may have longer tenures extending to several years.

Wholesale lending NBFCs are subject to regulatory oversight by the Reserve Bank of India (RBI) and other relevant authorities. They must comply with regulatory guidelines, including capital adequacy requirements and risk management practices.

Wholesale lending NBFCs may engage in loan syndication and co-lending arrangements with banks and other financial institutions to share the risk and provide larger loan amounts to borrowers.

Managing the asset-liability position is crucial for wholesale lending NBFCs to ensure they have the necessary liquidity to meet their obligations. They often employ sophisticated ALM strategies to maintain financial stability.

Some wholesale lending NBFCs specialize in serving specific industries, such as real estate, infrastructure, or healthcare. This specialization allows them to have in-depth knowledge of the unique requirements and risks associated with those sectors.

Risks Faced by Wholesale Lending NBFCs

All risks faced by a typical NBFC is faced by wholesale lending NBFC as well. However, there are some specific risks faced by the Wholesale Lending NBFC such as:

Concentration Risk: Too much concentration to a specific business segment or to a specific business group or significant portion of total portfolio to a single borrower or a single group. This may affect the NBFC adversely.

Economic and Industry Risk: Wholesale lending NBFCs are exposed to broader economic and industry-specific risks. Economic downturns, changes in industry conditions, or regulatory shifts can impact the credit quality of their borrowers.

Evergreening Risk: Typically, this risk is encountered in construction industry. It refers to a practice where a construction company engages in activities to artificially maintain or prolong the apparent health or performance of its projects or financial position. his practice can involve various actions that mask underlying issues or risks, ultimately leading to unsustainable or unhealthy financial conditions.

Regulatory Requirements on Wholesale Lending in India

RBI has issued various guidelines on NBFCs. Major ones focusing on Wholesale Lending are:

- Wholesale Lending NBFCs are required to maintain a minimum capital adequacy ratio (CAR) as specified by the RBI. Read latest ICAAP (Internal Capital Adequacy Assessment Process) norms.
- RBI has established exposure norms that limit the maximum exposure of Wholesale Lending NBFCs to a single borrower or group of related borrowers to mitigate concentration risk.
- Wholesale Lending NBFCs must adhere to RBI's guidelines on asset classification and provisioning. There is a prescribed ECL (Expected Credit Loss) provisioning based on IND AS 109
- NBFCs are expected to have adequate liquidity risk management systems in place, including maintaining a liquidity coverage ratio (LCR) as per RBI guidelines.
- Wholesale Lending NBFCs are required to have a Fair Practices Code (FPC) in place to ensure fair and transparent dealings with customers, including timely grievance redressal mechanisms.
- Wholesale Lending NBFCs must submit regular reports and disclosures to the RBI, including financial statements, asset-liability management (ALM) reports, and other regulatory filings.
- Wholesale Lending NBFCs are required to establish a robust risk management framework that includes credit risk, market risk, operational risk, and liquidity risk management.
- RBI guidelines require NBFCs to obtain and maintain external credit ratings for their debt instruments, and disclosure of these ratings is mandatory.
- RBI has specific guidelines for Wholesale Lending NBFCs engaged in securitization and asset reconstruction activities, including registration and compliance with securitization regulations.

Illustrative Key Focus Internal Audit Areas

1. **Scenario:** It is observed that there is Inconsistent adherence to credit risk policies and guidelines in the loan origination process

Focus: Internal Auditor should review the underwriting authority matrix, any list of accepted deviations and whether the MIS is created and presented to the management.

2. **Scenario:** It is observed that 33% of the loan portfolio is given to 15 companies, where there are common directors

   Focus: Internal Auditor should verify whether such transactions are approved by the board of directors of the Company and that there are no restrictions in the policy against such lending.

3. **Scenario**: It is observed that the NBFC extends a new loan to a borrower to cover the interest or principal repayment of an existing loan that the borrower is unable to service.

   Focus: Review loan approval processes to ensure new loans are not granted solely to pay off existing debt. Check for proper documentation and reasons for extending new loans.

4. **Scenario:** A lender modifies loan terms, such as extending the maturity date or reducing interest rates, to help a struggling borrower continue servicing the debt.

   Focus: Review loan modification policies and ensure they are followed consistently. Assess concealing Non-Performing Loans

5. **Scenario:** A NBFC classifies non-performing loans as performing loans on its financial statements to make its financial condition of borrowers before approving modifications. portfolio appear healthier than it is.

   Focus: Scrutinize the accuracy of loan classification and impairment assessment. Ensure compliance with regulatory reporting requirements.

6. **Scenario**: NBFC accepts collateral with inflated valuations to secure evergreen loans, creating a false sense of security.

   Focus: Review the collateral valuation process and assess the accuracy of valuations. Confirm that collateral values are periodically reassessed.

Retail Lending

3.2 Retail lending Non-Banking Financial Companies (NBFCs) are financial institutions that primarily focus on providing loans and financial

services to individual consumers or retail customers. Unlike wholesale lending NBFCs, retail lending NBFCs cater to the needs of individual borrowers.

Retail lending NBFCs specialize in serving the credit and financial needs of individual consumers. Their primary objective is to provide a wide range of financial products and services to meet the personal financing needs of retail customers.

The clients of retail lending NBFCs are individual consumers seeking financing for various purposes, such as purchasing homes, automobiles, consumer durables, funding education, meeting medical expenses, or addressing personal financial emergencies.

Retail lending NBFCs offer a variety of loan products tailored to the needs of retail borrowers. Common loan types may include home loans, personal loans, auto loans, education loans, two-wheeler loans, and consumer durable loans.

These NBFCs conduct risk assessments of individual borrowers to determine their creditworthiness. Credit scores, income verification, and other relevant factors play a crucial role in the lending decision process.

Interest rates for retail loans are usually determined based on factors such as the borrower's creditworthiness, prevailing market conditions, and the type of loan. Retail lending interest rates can vary widely between different loan products.

Loan tenures in retail lending can vary based on the type of loan. For example, personal loans may have shorter tenures (e.g., 1-5 years), while home loans often have longer tenures (e.g., 15-30 years).

While some retail loans may require collateral, such as a home or vehicle, retail lending NBFCs also offer unsecured loans. Unsecured loans do not require collateral but may have higher interest rates to compensate for the increased risk.

Retail lending NBFCs are subject to regulatory oversight by the relevant financial regulatory authorities in their respective countries or regions. Compliance with regulatory guidelines, including interest rate regulations and consumer protection laws, is essential.

Many retails lending NBFCs are adopting digital technologies to streamline loan origination, approval processes, and customer interactions. Digital lending platforms and mobile apps are becoming more common.

Effective risk management is crucial in retail lending. NBFCs in this sector use risk assessment tools, data analytics, and credit scoring models to manage credit risk and make informed lending decisions.

Retail lending NBFCs often focus on building strong customer relationships. Good customer service, transparent communication, and efficient grievance redressal mechanisms are essential for maintaining customer trust.

Some retail lending NBFCs actively work to promote financial inclusion by extending credit to underserved or unbanked segments of the population. They may offer microfinance or small-ticket loans to individuals with limited access to traditional banking services.

Risks Faced by Retail Lending NBFCs

All risks faced by a typical NBFC is faced by retail lending NBFC as well. However, there are some specific risks faced by the Retail Lending NBFC such as:

Customer Churn: Rapid customer turnover or attrition can impact the loan portfolio's stability.

Default Risk: Due to high volume of customers and lesser ticket size, intentional defaults may put strain on the entire portfolio.

Illustrative Key Focus Internal Audit Areas

Scenario: There is a considerable variance in sanctioning of loan.

Focus: Internal Auditor should review whether there is a target defined for loan sanction and there is an MIS prepared and presented to senior management by the function.

Scenario: During the review, it was noted that there is no evidence available for the trainings given to the recovery agents as required by RBI guidelines.

Focus: Internal Auditor should verify whether there have been many customer complaints and whether the clause for training is included in the agreement with recovery agency.

Illustrative Fraud Scenarios in Retail Lending

Here are some practical scenarios of frauds in retail NBFCs and what internal audits should check:

1. Identity Fraud: Customers may use false identities or forged documents to obtain loans or financial services. Internal audit should verify

the authenticity of customer identities and documents through rigorous KYC (Know Your Customer) procedures.

2. Loan Application Fraud: Individuals might submit fraudulent loan applications with inaccurate financial information. Internal audits should ensure that the underwriting process assesses the creditworthiness of applicants thoroughly.

3. Misappropriation of Funds: Employees or customers may siphon off funds from the NBFC through various means. Internal audit must regularly reconcile financial records and bank statements to detect any irregularities.

4. Embezzlement by Employees: Staff may misappropriate funds or manipulate records. Internal audits should include regular reviews of financial controls, segregation of duties, and internal reporting mechanisms to identify any unusual activities.

5. Loan Disbursement Fraud: There could be instances where loans are disbursed without proper collateral or documentation. Auditors should check the loan disbursement process to ensure compliance with policies and procedures.

6. Asset Misappropriation: Employees or customers might steal physical assets or misuse company resources. Internal audit should track and verify the physical assets of the NBFC.

7. Forgery and Fake Collateral: Customers might submit fraudulent collateral documents. Internal audit should verify the authenticity of collateral and conduct on-site inspections if necessary.

8. Cybersecurity Breaches: Retail NBFCs are vulnerable to cyberattacks, which can result in financial losses and data breaches. Auditors should assess the company's cybersecurity measures and response plans.

In addition to these scenarios, internal audit in retail NBFCs should also assess the adequacy of risk management processes, internal controls, and conduct regular reviews of loan portfolios to identify potential signs of fraud or credit quality deterioration. It's essential to stay updated with industry best practices and regulatory changes to adapt internal audit procedures accordingly.

Gold Loans

3.3 Gold loans have been a popular financial product in India, particularly in the Non-Banking Financial Company (NBFC) sector. These loans provide borrowers with quick access to funds by using their gold ornaments as collateral. However, NBFCs offering gold loans must navigate several risks and adhere to stringent regulatory requirements to ensure the stability of their operations and safeguard the interests of both lenders and borrowers. In this technical guide, we will explore the intricacies of gold loans in the NBFC sector, focusing on the top risks, regulatory requirements in India, and what internal audit should check while auditing gold loans.

Collateral: Gold loans are secured loans where borrowers pledge their gold ornaments, coins, or bars as collateral. The value of the loan is determined based on the purity and weight of the gold.

Quick Processing: One of the key attractions of gold loans is their quick processing time. NBFCs can disburse loans within minutes, making them a convenient option for borrowers in need of immediate funds.

Interest Rates: Interest rates for gold loans tend to be higher compared to traditional secured loans but lower than unsecured loans. The rates may vary among NBFCs.

Top Risks Faced by NBFCs in Lending Against Gold

Price Volatility: The value of gold can fluctuate significantly, which poses a risk to both the borrower and the NBFC. A sharp drop in gold prices can result in the borrower's collateral falling below the loan amount.

Quality of Gold: Ensuring the purity and quality of the gold offered as collateral is crucial. Counterfeit or impure gold can lead to losses for the NBFC.

Recovery Challenges: If borrowers' default on their gold loans, the NBFC must sell the gold to recover the outstanding amount. Efficient auction processes and price realization are critical.

Regulatory Compliance: NBFCs must comply with stringent regulations to prevent money laundering and fraud. Failure to do so can result in legal and reputational risks.

Regulatory Requirements in India

NBFCs shall implement the following when lending to individuals against gold jewellery.

They must implement board-approved lending against the gold policy that should, among other things, address the following:

Necessary measures to guarantee that the RBI's KYC regulations are followed, and that sufficient due diligence is done on the customer before granting any loan. NBFCs are required to establish the identity of borrowers and verify the source of the gold. This is to prevent illicit funds from being laundered through gold loans.

The Reserve Bank of India (RBI) sets the maximum LTV ratio for gold loans. Currently, it stands at 75%, meaning the loan amount cannot exceed 75% of the value of the gold.

Proper assaying methods for the received jewels.

Internal mechanisms for confirming ownership of the gold jewellery.

Ample systems for keeping the valuables in secure possession, ongoing system reviews, employee training, and surprise and periodic internal auditor inspections to make sure the procedures are strictly followed.

The jewels accepted as collateral should be properly insured.

In the event of non-repayment, the borrower should be given ample warning before the auction. There should be no conflicts of interest, and the auction process must guarantee that all transactions throughout the auction, including those with group firms and linked entities, are conducted on an arms-length basis. The process of auctioning gold in case of default is strictly regulated to ensure transparency and fair treatment of borrowers.

Public notice of the sale should be given by placing advertisements in at least two publications, one in the local language and one in a national daily newspaper.

The gold pledged will only be auctioned through auctioneers approved by the Board.

As a matter of policy, the NBFCs should refrain from taking part in the auctions themselves.

The policy shall also cover the systems and procedures to be put in place for dealing with fraud, including the separation of duties of mobilisation, execution, and approval.

The loan agreement must also include information on the auction process.

Illustrative Key Focus Internal Audit Areas

Compliance with Regulatory Guidelines

Scenario: An internal auditor discovers that the NBFC has disbursed gold loans exceeding the RBI-prescribed Loan-to-Value (LTV) ratio, allowing borrowers to receive loans worth 80% of the gold's value.

Focus: The audit should ensure that the NBFC complies with the LTV ratio set by the RBI to prevent excessive lending against gold. Check whether adequate system controls are built in to restrict LTV limit funding.

Quality of Collateral

Scenario: During an audit, it is revealed that the NBFC accepted gold jewellery without conducting proper assays to verify its purity, resulting in a significant portion of impure gold being held as collateral.

Focus: The audit should assess the procedures for evaluating the quality and purity of gold pledged as collateral to mitigate the risk of counterfeit or low-quality gold.

Risk Management

Scenario: The price of gold experiences a sharp decline, and the auditor observes that the NBFC hasn't adjusted its risk management strategies, leading to a higher risk of collateral value falling below the loan amount.

Focus: The audit should evaluate the NBFC's risk assessment and risk mitigation strategies, including periodic revaluation of collateral based on gold price movements.

Documentation

Scenario: During the audit, it is found that several loan agreements lack essential information, such as borrower details or terms and conditions, creating legal ambiguities.

Focus: The audit should review loan documentation to ensure that all necessary information is accurately recorded, helping to avoid legal disputes and ensure compliance.

Auction Process

Scenario: The internal auditor observes that the NBFC lacks a transparent and well-documented process for auctioning gold in the event of loan defaults, potentially leading to disputes with borrowers.

Focus: The audit should assess the auction procedures to guarantee fairness, transparency, and compliance with regulatory requirements, reducing the risk of disputes and losses during recovery.

Interest Rate Caps

Scenario: The audit identifies that the NBFC has charged interest rates on gold loans exceeding the RBI-prescribed caps.

Focus: The audit should verify that the NBFC complies with interest rate caps set by the company and regulatory authorities to ensure fair and lawful lending practices.

Know Your Customer (KYC) Compliance

Scenario: During an audit, it is discovered that the NBFC did not adequately verify the identity and source of funds of certain borrowers.

Focus: The audit should scrutinize the NBFC's KYC procedures to confirm that they are rigorous and comprehensive, reducing the risk of fraudulent transactions and money laundering.

Customer Communication and Transparency

Scenario: An internal audit reveals that the NBFC has not adequately communicated the terms and conditions of gold loans to borrowers, leading to confusion and dissatisfaction among customers.

Focus: The audit should assess customer communication practices to ensure borrowers are well-informed about loan terms, interest rates, repayment schedules, and potential risks.

Default Management

Scenario: The NBFC lacks a well-defined strategy for managing loan defaults, resulting in delays in initiating the recovery process and increased credit risk.

Focus: The audit should review the default management procedures to ensure timely action in the event of loan defaults, including legal actions, if necessary, to minimize credit losses.

Gold Storage and Security

Scenario: During the audit, it is found that the NBFC does not have adequate security measures in place to protect the physical gold collateral stored in its premises, exposing it to theft or damage.

Focus: The audit should assess the security and storage protocols to safeguard the physical gold collateral, reducing operational risks.

Data Security and Privacy

Scenario: The internal audit uncovers vulnerabilities in the NBFC's data security, potentially exposing borrower information to data breaches.

Focus: The audit should review data security measures, including encryption, access controls, and compliance with data protection regulations, to protect sensitive customer data.

Fraud Prevention

Scenario: An audit identifies irregularities in loan disbursements, suggesting potentially fraudulent activities within the lending process.

Focus: The audit should investigate fraud prevention mechanisms, including employee training, fraud detection tools, and transaction monitoring, to mitigate the risk of fraudulent activities.

Portfolio Diversification

Scenario: The NBFC primarily focuses on lending against a single type of gold collateral, such as jewellery, without diversifying its portfolio.

Focus: The audit should assess the portfolio diversification strategy to reduce concentration risk and ensure a more balanced lending portfolio.

Market Research and Competitor Analysis

Scenario: The NBFC does not regularly monitor market trends and competitor offerings, potentially missing out on opportunities for product innovation or competitive pricing.

Focus: The audit should evaluate the NBFC's market research and competitor analysis processes to ensure it remains competitive and responsive to market changes.

Micro-finance

3.4 Microfinance is a vital financial service that caters to the needs of low-income individuals and small entrepreneurs who lack access to traditional banking services. In the NBFC (Non-Banking Financial Company) sector, microfinance has gained prominence as a product offering due to its potential for financial inclusion and poverty alleviation. NBFCs engaged in microfinance provide small loans, savings, insurance, and other financial services to economically vulnerable segments of society.

Small Ticket Size: Microfinance loans typically have a small ticket size, making them accessible to low-income borrowers.

Group Lending: Many NBFCs use the group lending model, where borrowers form small groups, and the group is collectively responsible for loan repayment. This social collateral helps mitigate credit risk.

Personalized Service: Microfinance NBFCs often employ field officers who visit borrowers regularly, fostering a closer relationship and ensuring better repayment rates.

Key Risks Faced by NBFCs in Lending to MFIs

Credit Risk: The primary risk is the creditworthiness of borrowers. MFIs often serve individuals with limited credit histories, making it challenging to assess their ability to repay loans. Credit risk also looks at whether credit policies and procedures are correctly followed and administered by staff and whether credit transactions are properly recorded in your MFI's loan tracking system and correctly summarized and presented in the financial and portfolio reports.

Operational Risk: MFIs often operate in remote and challenging environments, which can lead to operational challenges such as difficulties in loan disbursement and collection.

Regulatory Risk: Changes in regulatory policies can impact the operations of NBFCs involved in microfinance. Adherence to regulatory guidelines is crucial to mitigate this risk.

Market Risk: Economic downturns or regional factors can affect the repayment capacity of borrowers, leading to increased defaults.

Liquidity Risk: Managing the cash flow and liquidity needs of the NBFC while meeting the demands of borrowers can be challenging.

Fraud Risk: Intentional or deliberate deception for unfair or unlawful personal gain. These are intentional actions, manipulation of data or documents, or the abuse of office, policies, procedures, or documents of MFI's property for the purpose of personal gain.

Security Risk: Risk of theft or harm to property or person. MFIs – both large and small -- are about people, paper and money. Money, particularly the high use of cash in most MFIs, creates a high risk for security of both money and people. While the move to electronic banking and money transfers is still lagging in most parts of the world, this technology will greatly minimize

security risks on the issue of money. It will of course increase new risks related to electronic transactions.

Regulatory Requirements in India

In India, microfinance NBFCs are subject to regulatory oversight by the Reserve Bank of India (RBI) and other relevant authorities. The Reserve Bank has issued Reserve Bank of India (Regulatory Framework for Microfinance Loans) Directions, 2022 for regulating microfinance loans. The Directions will come into force from April 01, 2022. Refer link https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12256&Mode=0

Uniform regulatory framework for all entities extending micro finance loans: Directions cover all entities that provide microfinance loans i.e. the applicability is dependent on the nature of loans granted by any entity, irrespective of the type of entity or end-use of the loan. Earlier only NBFC-MFIs were subject to microfinance specific regulations.

Assessment of Household income: The definition of annual household income has been modified to only keep a uniform household income limit (increased from the earlier limits).

Removal of interest rate cap: One of the major changes is that the interest rate ceiling has been removed, which was earlier applicable on NBFC-MFIs.

Conditions for the loan: Earlier, there was a maximum cap on the amount of loan as well as on the number of NBFC-MFI that could grant microfinance loans to a borrower. Now microfinance loans can be granted up to a maximum limit calculated as a percentage of the household income of the borrowers.

Stricter regulatory framework w.r.t. recovery methods, fair practices code, etc.

Illustrative Key Focus Internal Audit Areas

Auditing microfinance loans in a Non-Banking Financial Company (NBFC) involves assessing various key areas to ensure compliance, risk mitigation, and operational efficiency. Here are some practical scenarios and what internal audit should check:

Non-Performing Assets (NPAs)

Scenario: During the audit, Internal Auditor notices an increase in non-performing loans (NPLs) in a particular region.

Approach: Internal audit should investigate the cause of the rising NPLs, conduct a thorough review of the loan origination and approval process to identify weaknesses. This may involve examining credit risk assessment, due diligence, and collection procedures and loan monitoring practices to identify weaknesses and recommend improvements.

Interest Rate Management

Scenario: During the audit, internal auditor observers that the NBFC adjusts its interest rates in response to market changes

Approach: internal Auditor must assess whether the institution's interest rate changes are transparent and fair to borrowers, in accordance with regulatory requirements. Reviewing the transparency of interest rate disclosure to borrowers is also crucial.

Client Data Security

Scenario: During walkthrough of the process, internal auditor observes that the NBFC collects sensitive customer information for loan processing potentially exposing client information.

Approach: Internal audit should verify that data protection policies are in place, and customer data is securely stored and accessed only by authorized personnel. Also assess data protection protocols, including IT systems and employee training, to identify and mitigate security risks**.**

Liquidity Management

Scenario: Internal auditor during audit observes that the NBFC has insufficient liquidity to meet loan disbursement and withdrawal demands.

Approach: Internal audit must assess the institution's financial sustainability by analyzing its income sources, expenses and liquidity risk management framework, including stress testing, to ensure the NBFC can meet its obligations under different scenarios and recommend strategies for long-term viability.

Credit Risk Assessment

Scenario: Internal auditor observers that the NBFC relies on credit scoring models for loan approvals which is not reviewed timely and updated timely leading to a high default rate.

Approach: Audit should scrutinize the NBFC's credit scoring and underwriting process to review its accuracy and effectiveness and ensure they are adapted to the target market's characteristics.

Fraud Prevention and Detection

Scenario: An employee is suspected of embezzling funds from microfinance accounts.

Approach: Internal audit should verify the process in place to identify irregularities. Review the controls instituted for fraud prevention, detection and reporting and recommend stronger internal controls to prevent fraud.

Customer Grievance Handling

Scenario: Clients are expressing dissatisfaction with loan terms and repayment schedules.

Approach: Audit should evaluate the NBFC's complaint handling procedures and recommend improvements to ensure timely and fair resolution of customer issues.

Technology and Digital Services

Scenario: The institution is transitioning to digital financial services.

Approach: Audit should assess IT controls, cybersecurity, and the effectiveness of the digital service delivery channels.

Equipment Finance

3.5 India has experienced significant economic growth over the past few decades, resulting in increased demand for various types of equipment across industries such as manufacturing, construction, agriculture, healthcare, and transportation.

India's infrastructure development, including roads, railways, airports, and ports, has been a key driver of the need for equipment financing. These projects require a wide range of machinery and vehicles.

Different industries have unique requirements for equipment. For example, the healthcare sector needs medical equipment, while the construction sector requires heavy machinery. Many big capital-intensive industries like Steel and Auto Giants are supported heavily by various small ancillary industries, which require various equipment.

Rapid technological advancements in equipment have shortened their lifecycle, increasing the need for flexible financing options.

Traditional banks may be cautious about financing equipment, particularly for SMEs with limited collateral. Equipment Finance NBFCs fill this financing gap by offering specialized equipment loans and leases.

Equipment finance is asset-centric, i.e. equipment itself serves as collateral. This reduces credit risk for lenders.

Equipment Finance NBFCs can tailor financing solutions to meet the unique needs of various industries, allowing businesses to acquire equipment without significant upfront costs.

By enabling businesses to access the equipment they need, Equipment Finance NBFCs contribute to economic growth and infrastructure development. This, in turn, generates employment opportunities and stimulates related industries.

Equipment Finance NBFCs can focus on specific industries or sectors, gaining in-depth knowledge and specialization, which benefits borrowers by offering industry-specific insights and solutions.

These NBFCs often provide flexibility in terms of lease durations, payment structures, and end-of-term options, allowing businesses to align financing with their cash flow and equipment needs.

Many Equipment Finance NBFCs have embraced digitalization and technology to streamline loan origination, servicing, and customer interactions, providing a more efficient borrowing experience.

Key Risks in Equipment Finance

All risks faced by a typical NBFC is faced by equipment finance NBFC as well. However, there are some specific risks such as:

Asset Risk: The value of the equipment or asset being financed can depreciate over time. Equipment finance companies must assess and manage the risk associated with asset depreciation and the potential for residual value losses.

Economic Cycles Risk: The equipment finance industry is sensitive to economic cycles. During economic downturns, businesses may delay or cancel equipment purchases, affecting the financing sector.

Recovery of Defaulted Assets: In cases of loan defaults, repossessing and selling equipment to recover losses can be a complex and time-consuming process.

Illustrative Key Focus Internal Audit Areas

Scenario: Of the 10 sampled lending, there was no evidence of an on-site inspection and appraisal of the equipment in 5 cases.

Focus: IA should look at alternate methods to verify existence and valuation of the equipment, also it should ensure an automated check where loan amount is not disbursed unless there is an approval from appropriate authority that the inspection has happened.

Scenario: On physical verification of an NPA case, it was observed that the equipment is lying in a packed condition thereby the borrower is not using the equipment as a result of which there is no revenue generated on account of that equipment and finally borrower is not paying instalment.

Focus: IA should recommend recovery of the equipment and auction. Also, in future a detailed analysis of usage plan / business plan with collaborative proof such as orders in hand etc. should be carried out by business before underwriting such loans.

Consumer Durables and Two Wheelers

3.6 A Consumer Durable NBFC in India is a specialized financial institution that primarily focuses on providing financing solutions for the purchase of consumer durables such as electronics, appliances, furniture, two-wheelers, and other high-value items. These NBFCs play a crucial role in making these products more accessible and affordable to a wide range of consumers.

Over the years, consumer preferences have shifted towards purchasing consumer durables such as electronics, appliances, furniture, and vehicles. These items are considered essential for improving the quality of life. Economic growth and increasing disposable income levels have empowered consumers to aspire to own high-value consumer durables that were previously out of reach.

The retail landscape has evolved with the emergence of modern retail chains, e-commerce platforms, and specialized consumer durable stores, offering a wide range of choices to consumers.

Traditional banks may have limitations in providing specialized financing for consumer durables. Consumer Durable NBFCs bridge this gap by focusing exclusively on offering financing solutions for consumer durable purchases. Consumer Durable NBFCs make it possible for individuals and households to access high-value consumer durables without making large upfront payments, thus enhancing affordability.

Consumer Durable NBFCs specialize in offering financing options tailored to the purchase of consumer durables. This can include loans, leases etc. hey typically cover a diverse range of consumer durables, including but not limited to, televisions, refrigerators, washing machines, air conditioners, smartphones, laptops, furniture, and two-wheelers.

These NBFCs provide consumers with flexible financing solutions, including equated monthly instalments (EMIs), zero or low-down payments, and customized repayment terms. Consumer Durable NBFCs often collaborate with manufacturers, retailers, and dealerships to offer consumers attractive financing deals, promotional offers, and easy access to credit at the point of sale.

These NBFCs often offer schemes where customers can enjoy interest-free or low-interest financing for a specific period, contributing to increased affordability. By providing financing options to a broad spectrum of customers, including those without access to traditional banking services, Consumer Durable NBFCs contribute to financial inclusion.

Key Risks Faced in Consumer Durables and Two Wheelers

All risks faced by a typical NBFC is faced by consumer durables and two-wheeler financing NBFC as well. Major being:

Credit Risk: Inaccurate or inadequate credit risk assessment may result in loans being extended to customers with a higher likelihood of default. Borrowers may default on their loan or lease payments, leading to financial losses for the lender.

Asset Risk: The value of consumer durables and two-wheelers can depreciate rapidly, affecting the collateral's value in case of default. Estimating the future residual value of assets accurately is crucial for determining loan or lease terms.

Market Risk: Changes in consumer preferences and market demand for specific consumer durables and two-wheeler models can impact the resale value of financed assets.

Legal Risk: Disputes related to loan agreements, asset repossession, or recovery processes can result in legal challenges. Ensuring compliance with laws related to the collateral (such as vehicle registration) is essential to protect organisation’s interests.

Sustainability Risk: Changes in environmental regulations may affect the resale value of certain assets, especially if they do not meet updated standards.

Illustrative Key Focus Internal Audit Areas

1. Scenario: The company's LTV ratios for various consumer durables are uniform and do not account for variations in asset depreciation or specific market conditions.

Focus: IA should focus on verifying whether different parameters are used for different product segment while determining LTV. IA should recommend implementing dynamic LTV ratios that consider asset depreciation rates and specific market conditions, ensuring that loan terms align with the true asset value.

2. Scenario: In some cases, there were gaps in documenting the collateral, including vehicle registration and ownership details. There were no supporting documents confirming the ownership of the vehicle.

Focus: IA should verify and make sure that the establishing ownership is a mandatory step while disbursing the loan amount. In case there is a delay in registration of vehicle in borrower's name a penalty should be levied beyond defined tolerance limit.

Loan Against Securities

3.7 Loan Against Securities (LAS) is a type of loan offered by Non-Banking Financial Companies (NBFCs) and banks, where individuals or entities can pledge their financial securities (like stocks, bonds, mutual funds) as collateral to obtain a loan.

Here's how it works:

Pledging Securities: The borrower provides their securities to the lender as collateral. These securities are kept in a demat account or a designated account under the lender's control.

Loan Approval: The lender evaluates the value and quality of the securities and approves a loan amount based on a percentage of the securities' market value. The loan-to-value (LTV) ratio typically varies depending on the type of securities.

Terms and Interest: The lender specifies the terms of the loan, including the interest rate, repayment schedule, and other conditions.

Use of Loan Proceeds: Borrowers can use the loan proceeds for various purposes, such as personal expenses, investments, or business needs.

Key Risks Faced in Lending Against Securities

Key risks faced by NBFCs in Lending Against Securities and mitigation strategies:

Market Risk: The value of securities can fluctuate, potentially falling below the loan amount. To mitigate this, lenders regularly monitor the market value of pledged securities and may require additional collateral if needed.

Credit Risk: Borrowers may default on their loans. To mitigate this, lenders assess the creditworthiness of borrowers and set appropriate LTV ratios. They may also require borrowers to maintain a margin in case the value of pledged securities falls.

Operational Risk: Errors or fraud in handling securities can lead to losses. NBFCs should have robust operational processes and controls in place to prevent and detect such issues.

Liquidity Risk: In case of a sudden need to sell pledged securities, the lender may face challenges. Lenders maintain liquidity buffers and have contingency plans to address this risk.

Illustrative Key Focus Internal Audit Areas

Assessment of Risk Management: Ensure that the NBFC has a comprehensive risk management framework in place to identify, assess, and mitigate the risks associated with LAS.

Valuation and Monitoring: Review the methods used for valuing pledged securities and assess the frequency and effectiveness of monitoring their market value.

Compliance with Regulations: Ensure that the NBFC complies with all relevant regulations and guidelines related to LAS, including prudential norms and disclosure requirements.

Regulations with Respect to Loan Against Securities

The regulations governing LAS can vary by country and may change over time. In India, for example, the Reserve Bank of India (RBI) and Securities

and Exchange Board of India (SEBI) have issued guidelines and regulations for LAS. NBFCs are required to adhere to these guidelines, which cover aspects like LTV ratios, margin maintenance, and disclosure requirements.

It's important to consult the specific regulations applicable in your jurisdiction for detailed information on LAS requirements.

Non-Banking Financial Companies (NBFCs) typically monitor market risk in Loan Against Securities (LAS) through a combination of ongoing processes and risk management measures. Here's how they typically do it:

Regular Valuation: NBFCs regularly assess the market value of the securities pledged by borrowers. This valuation can be daily, weekly, or at other specified intervals, depending on the terms and risk assessment of each loan. Automated systems may be used to calculate the value based on market prices.

Loan-to-Value (LTV) Ratios: NBFCs set LTV ratios, which determine the maximum loan amount a borrower can receive relative to the market value of their pledged securities. These ratios are designed to provide a cushion against market fluctuations. If the market value of pledged securities falls below a certain threshold, the NBFC may require the borrower to provide additional collateral to maintain the required LTV ratio.

Margin Calls: When the market value of pledged securities approaches the LTV limit, NBFCs may issue margin calls to borrowers. This means the borrower is required to deposit additional securities or repay a portion of the loan to maintain the required margin. Failure to comply with margin calls could lead to liquidation of the pledged securities.

Stress Testing: NBFCs may conduct stress tests on their LAS portfolio to assess how it would perform under adverse market conditions. This helps them understand potential vulnerabilities and make adjustments to their risk management strategies accordingly.

Risk Models: Many NBFCs use sophisticated risk models and analytics to evaluate the risk associated with different types of securities and portfolios. These models consider factors such as historical price volatility, liquidity, and correlation with market indices.

Diversification: Diversifying the LAS portfolio by accepting a variety of securities from different sectors and asset classes can help mitigate concentration risk. This reduces the impact of adverse market movements on the overall portfolio.

Regulatory Compliance: NBFCs must adhere to regulatory guidelines related to LAS, which often include specific risk management requirements. These guidelines may mandate minimum LTV ratios, margin maintenance, and reporting standards.

Market Research: Continuous monitoring of market trends and economic indicators helps NBFCs anticipate potential market movements and make informed decisions regarding their LAS portfolio.

Reporting and Disclosure: Transparency is crucial in managing market risk. NBFCs are required to disclose information related to their LAS portfolio in their financial statements, including the composition of pledged securities, LTV ratios, and any significant changes in market risk exposure.

Internal Audit and Compliance: Regular internal audits and compliance checks ensure that the NBFC's risk management practices align with its policies and regulatory requirements.

Lending Against Securities

3.8 During an internal audit of lending against securities (LAS) in a Non-Banking Financial Company (NBFC), auditors focus on various key areas to ensure compliance, risk management, and operational effectiveness.

Illustrative Key Focus Internal Audit Areas

Here are some practical scenarios that illustrate these key areas of focus:

1. Risk Assessment and Underwriting

Scenario: An NBFC has approved LAS loans with high loan-to-value (LTV) ratios, close to regulatory limits.

Key Focus: Auditors assess the risk assessment and underwriting process to ensure compliance with regulatory guidelines regarding LTV ratios. They review whether proper due diligence was conducted, and if deviations from standard LTV ratios were adequately justified.

2. Valuation and Monitoring

Scenario: The market value of certain pledged securities has declined significantly, approaching or falling below the required LTV ratio.

Key Focus: Auditors should examine the process for monitoring pledged securities' market values and issuing margin calls to borrowers. They should verify if margin calls were made promptly and that actions were taken to mitigate market risk.

3. Documentation and Legal Compliance

Scenario: The NBFC lacks complete and updated documentation for some LAS loans.

Key Focus: Auditors ensure that all required documentation, including loan agreements, security creation documents, and KYC checks, are in place and up to date. They should verify if the NBFC complies with legal requirements.

4. Concentration Risk Management

Scenario: The NBFC has a significant concentration of LAS loans in a particular industry sector.

Key Focus: Auditors assess the concentration risk and evaluate whether the NBFC has implemented strategies to mitigate this risk, such as diversification of collateral types or sectors.

5. Operational Controls and Processes

Scenario: There are instances of discrepancies in the reconciliation of pledged securities.

Key Focus: Auditors should review the operational controls and processes related to handling pledged securities. They should ensure that reconciliation processes are robust and that discrepancies are promptly investigated and resolved.

6. Regulatory Compliance

Scenario: The NBFC is not adhering to the regulatory guidelines related to LAS.

Key Focus: Auditors check for compliance with regulations governing LAS, including loan classification, provisioning, and disclosure requirements. They ensure that the NBFC follows all regulatory norms.

7. Stress Testing

Scenario: The NBFC has not conducted stress tests on its LAS portfolio.

Key Focus: Auditors should recommend or assess the stress testing conducted by the NBFC to evaluate how the portfolio would perform under adverse market conditions. They should verify whether the NBFC has taken corrective actions based on the results of stress tests.

8. Credit Risk Management

Scenario: Borrowers are consistently missing margin calls.

Key Focus: Auditors should evaluate the NBFC's credit risk assessment of borrowers and examine whether policies and procedures are in place to address delinquent borrowers, including collateral liquidation processes.

9. Reporting and Disclosure

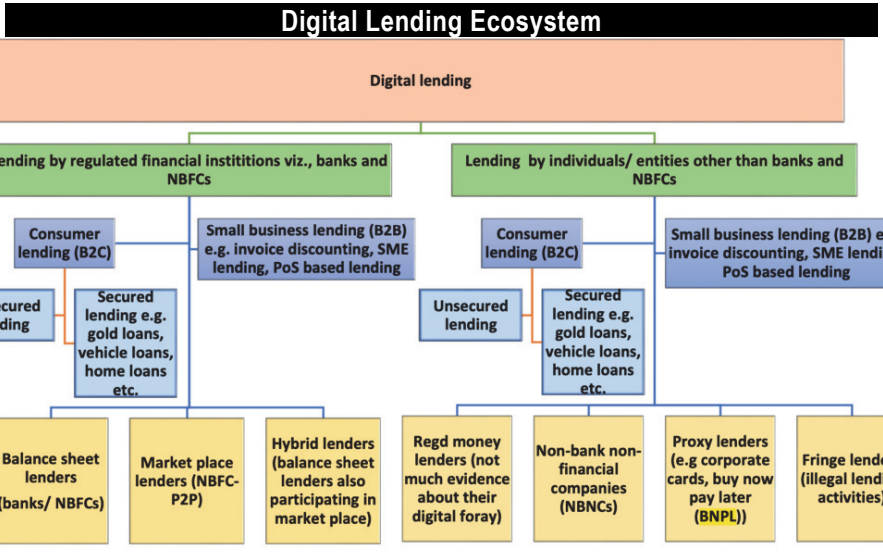
Scenario: The NBFC lacks transparency in reporting its LAS portfolio's composition.

Key Focus: Auditors should review the adequacy and accuracy of reporting and disclosure related to LAS loans in financial statements and other reports, ensuring transparency for stakeholders.

Fintech/ Digital Lending

3.9 Digital lending is the service of providing loans and credit facilities with the help of online platforms, digital technologies and data analytics by assessing a borrower's creditworthiness, and thus approving and disbursing funds. It is fast becoming a popular mode of credit delivery in the context of increasing digital connectivity, services, and the culture of digital finance.

According to the RBI, "Digital lending is a remote and automated lending process, largely by use of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service." Unlike in the case of physical lending, largescale use of digital technologies is to be used to qualify a lending as digital lending.



Following are the main features and elements of digital lending.

Use of Online Platforms: Digital lending platforms are typically web-based or mobile applications that allow borrowers to apply for loans, submit necessary documentation, and track the status of their loan applications.

Use of Data Analytics: Digital lending platforms rely on advanced data analytics and algorithms to assess a borrower's creditworthiness, based on various factors such as credit history, income, employment, and social media presence. This process helps in making more accurate and faster lending decisions.

Automated Processes: Digital lending platforms use automation to streamline various processes involved in loan origination, approval, and disbursement. This can significantly reduce the time taken for loan approval and disbursement.

Paperless Transactions: Digital lending eliminates the need for physical paperwork, as all transactions and document submissions occur online. This not only makes the process more convenient but also reduces the chances of errors and fraud.

Personalized Services: Digital lending platforms can offer personalized loan products and interest rates based on a borrower's individual needs and credit profile. This can lead to more attractive loan offers and a better borrowing experience.

Increased Access: Digital lending platforms are accessible 24/7, allowing borrowers to apply for loans at their convenience. Moreover, these platforms can cater to borrowers with diverse credit profiles, including those with limited or no credit history.

Regulatory Compliance: Digital lending platforms are subject to the same regulations as traditional financial institutions, including anti-money laundering (AML) and know-your-customer (KYC) requirements. They must adhere to these regulations to ensure the security and privacy of users' data and maintain the integrity of the financial system.

Regulatory Initiative by the RBI on Digital Lending

For the Regulated Entities (RE), detailed guidelines including customer protection, assessment of creditworthiness of the customers, data usage, management of loss etc. are also provided under the RBI regulation.

RBI's new digital lending regulation is applicable for the Regulated Entities

While leaving the responsibility of regulating the unregulated entities under central government rules, the RBI has elaborated basic and entry level guidelines for regulating the digital lending activities of the regulated entities. All Commercial Banks, Primary (Urban) Co-operative Banks, State Co-operative Banks, District Central Co-operative Banks; and Non-Banking Financial Companies (including Housing Finance Companies) are regulated (these are called Regulated Entities) by the RBI and hence the new digital lending regulation is applicable for this group.

Does any physical interaction mean non-digital lending?

Even if a minimum level of physical interaction is made while delivering digital lending, it can be counted as digital lending according to the RBI guidelines. There are different stages for lending – customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service etc.

According to the RBI regulations, there should be the use of seamless digital technologies 'largely' to be qualified for Digital Lending definition. Still, there is operational flexibility to regulated entities in 'Digital Lending'. Hence, even if some physical interface with customer is made, the lending will qualify for the definition of Digital Lending.

There are other players in the digital lending process- the two prominent players are the Lending Service Provider (LSP) and Digital Lending Apps/Platforms (DLAs). These are the entities who provide digital lending services on behalf of regulated entities like NBFCs.

Lending Service Provider (LSP)

LSP is an agent of a Regulated Entity who carries out one or more of lender's functions or part thereof in customer acquisition, underwriting support, pricing support, servicing, monitoring, recovery of specific loan or loan portfolio on behalf of REs in conformity with extant outsourcing guidelines issued by the Reserve Bank.

Digital Lending Apps/ Platforms (DLAs)

The Digital Lending Apps are mobile and web-based applications who have the user interface for facilitating digital lending services. DLAs also includes apps of the Regulated Entities (REs) as well as those operated by Lending

Service Providers (LSPs) engaged by REs for extending any credit facilitation services as per the guidelines given by the RBI.

The RBI guidelines reiterate that any outsourcing by an RE to an LSP or a DLA does not diminish the RE's obligations to conform to the existing RBI guidelines on outsourcing. In addition, REs also needs to ensure that LSPs and DLAs comply with the guidelines.

A. Customer Protection and Conduct Requirements **To enhance customer awareness and protect the interests of customers, RBI has issued guidelines on customer protection and conduct requirements. Key aspects of the guidelines are as follows:**	
Areas covered in the guideline	Detailed guidance
Loan disbursal, servicing and repayment directly through RE account	To enhance transparency in a digital lending transaction, REs need to ensure that all disbursements are made to a bank account of the borrower without any pass-through account/pool account of any third party (including LSPs/DLAs)7. Similarly, all repayments, etc. should be executed by a borrower directly in a RE's bank account.
Collection of fees, charges, etc.	Fees/charges: The REs should directly pay the fees, charges, etc. that are payable to LSPs, and these should not be charged by the LSP to the borrower directly. Penal interest/charges: The penal interest/charges levied on the borrower should be based on the outstanding amount of the loan. Further, the rate of the penal charge should be disclosed on an annualised basis to the borrower in the Key Fact Statement.
Enhanced disclosures to the borrowers	REs need to ensure that the following information is available to the borrowers: • Key fact statement: Before execution of the contract for any digital lending product, REs should provide the borrower a Key Fact Statement (KFS) in a format prescribed by the guidelines. It is to be noted that any fees, charges, etc. which are not mentioned in the KFS cannot be charged by the REs to the

	borrower at any stage during the term of the loan. • Digitally signed documents: Upon execution of the loan contract, all documents (on the letterhead of the RE) signed by the borrower using digital signature should automatically flow to the borrower on his/her verified email/phone number. • List of LSPs: REs are required to prominently publish on their website their DLAs, LSPs engaged by them and the DLAs of such LSPs, with the details of activities for which they have been engaged. • Product information: The DLAs of the REs and/or of the LSPs engaged by the REs should prominently display information relating to the product features, loan limit and cost, etc. at the on-boarding/sign-up stage. • Link to website: The DLAs of the REs and of the LSPs engaged by the REs should have links to the REs' website where detailed information about the loan products, the LSPs, customer care, link to Sachet Portal, privacy policies, etc. is provided. Such information should be placed at a prominent single place on the website of the RE for ease of accessibility.
Grievance redressal	The responsibility of grievance redressal would remain with the RE. The guidelines have prescribed the following: • Nodal grievance redressal officer: LSPs of the REs should have a suitable nodal grievance redressal officer to deal with digital lending related complaints/issues raised by the borrowers against their DLAs. Contact details of the grievance redressal officer should be displayed and facility for lodging complaint should be made available on the DLA and websites of the RE and LSPs. • Reserve Bank-Integrated Ombudsman Scheme (RB-IOS): If any complaint lodged by a borrower against an RE or an LSP engaged by the RE is not resolved

	within the stipulated period (currently 30 days), he/she can lodge a complaint under the RB-IOS or as per any other grievance redressal mechanism prescribed by RBI.
Cooling-off/look-up period	The guidelines require borrowers to be given an explicit option to exit digital loans by paying the principal and proportionate Annual Percentage Rate (APR), without any penalty during this period- this is referred to as the cooling-off/look-up period. The period should be determined by the Board of Directors (Board) of the RE. Borrowers that continue with the loan even after the cooling-off period, prepayment would continue as per the current RBI guidelines
Assessing borrower's creditworthiness	With a view to restrict reckless lending and prevent over-indebtedness of the borrowers, the guidelines require REs to: • Capture the economic profile of the borrowers (covering age, occupation, income, etc.) to assess the borrower's creditworthiness in an auditable way, before digital loans can be extended to him/her through the DLA of the RE or of the LSP. • Ensure there is no automatic increase in credit limit unless explicit consent of the borrower is taken on record for such increase.
Due diligence and other requirements with respect to LSPs	The guidelines require REs to conduct enhanced due diligence before entering into a partnership with an LSP for digital lending, considering its technical abilities, data privacy policies, storage systems, fairness in conduct with borrowers and ability to comply with regulations and statutes. A periodic review of the conduct of the LSPs should be carried out by the REs. With regard to LSPs acting as recovery agents, REs should impart necessary guidance to such LSPs so that they discharge their duties responsibly and comply with the existing instructions in this regard

B. Technology and Data Requirement **In order to safeguard against the concerns relating technology and data requirement, the guidelines specifically provide following guidance:**	
Area covered in the guideline	Detailed guidance
Collection, usage and sharing of data with third parties	With regard to personal information of borrowers, the REs should ensure the following: • Need-based data: The collection of data by the DLAs of the REs and of the LSPs engaged by the REs should be need-based and with prior and explicit consent of the borrower having audit trail. • Access to apps: DLAs should desist from accessing mobile phone resources like file and media, contact list, call logs, etc. A one-time access can be taken with the consent of the borrower for camera, microphone, location or any other facility necessary for the purpose of e-KYC requirements. • Borrower to manage data: Borrower should be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/forget the data. • Purpose of obtaining consent: The purpose of obtaining borrower's consent needs to be disclosed at each stage of interface with the borrowers. • Sharing personal information: Explicit consent of the borrower should be taken before sharing personal information with any third party, except where such sharing is as per statutory/regulatory requirement.
Storage of data	With regard to storage of customer data, REs should ensure the following: Storage of minimal data: The LSPs/DLAs engaged by the REs should store only the basic minimal data that may be required to carry out their operations. The ultimate responsibility of customer's personal information and security will be that of the RE.

	Biometric data: No biometric data should be collected/stored in the systems associated with the DLA of REs/their LSPs unless allowed under existing statutory guidelines. Policy guidelines for storage of data: As multiple players have access to sensitive consumer/ financial data, clear policy guidelines regarding storage of customer data, such as type of data that can be stored, length of time it can be stored, etc. should be put in place and disclosed on the apps and website of the DLAs of the REs and of the LSPs engaged by the REs. Servers in India: All data should be stored in servers located within India.
Comprehensive privacy policy	The REs should ensure that their DLAs and LSPs engaged by them have a comprehensive privacy policy, which is compliant with applicable laws, associated regulations and RBI guidelines. It should also include details of third parties allowed to collect personal information through the DLA. This privacy policy should be made available publicly. These privacy policies should be disclosed at the time of access and collection of personal information of borrowers.
Technology standards	The REs should ensure that the REs and the LSPs engaged by them comply with various technology standards/requirements on cybersecurity stipulated by RBI and other agencies as specified from time to time. This will help to weed out non-serious players and push the sector towards maturity

C. Regulatory Framework:

From a regulatory perspective, RBI has prescribed the following requirements for digital lending:

Area covered in the guideline	Detailed guidance
Reporting to CICs	The REs should ensure that any lending done through their DLAs and/or DLAs of LSPs engaged by them is reported to Credit Information Companies (CICs) irrespective of its nature/tenure. Reporting

	would also be done for structured digital lending products extended by REs or LSPs engaged by REs over a merchant platform involving short-term, unsecured/secured credits or deferred payments (such as Buy Now Pay Later). Reporting should be done in accordance with the existing regulations. Submission of such information will break the perpetuation of data marginalisation of certain vulnerable groups. This will ensure less dependence on alternative data for financial consumers as more and more of them would develop formal credit history for themselves. Further, it will offer wider choices/competitive pricing for consumers.
Loss sharing arrangement in case of default	Various LSPs provide certain credit enhancement features such as first loss guarantee up to a pre-decided percentage of loans generated by it. From the LSP's perspective, offering First Loss Default Guarantee (FLDG) acts as a demonstration of its under-writing skills whereas from the RE's perspective, it ensures the LSP's skin in the business. For all practical purposes, credit risk is borne by the LSP without having to maintain any regulatory capital. The loan portfolio backed by FLDG is akin to off-balance sheet portfolio of the LSP wherein the nominal loans sit in the books of the lender without having to partake in any lending process. With increasing share of digital lending in retail/personal space, there is a potential for risk build-up because of these platforms. In this view, RBI has specified that RE shall ensure that total amount of DLG cover on any outstanding portfolio which is specified upfront shall not exceed five per cent of the amount of that loan portfolio. In case of implicit guarantee arrangements, the DLG Provider shall not bear performance risk of more than the equivalent amount of five per cent of the underlying loan portfolio. Further RE shall invoke DLG within a maximum overdue period of 120 days, unless made good by the borrower before that.

Illustrative practical scenario explaining some of the key area to focus during internal audit of Digital Lending Business

Scenario: NBFC "ABC" is engaged in the business of digital lending with tie up with multiple lending service providers (LSP's) who provide loans to borrowers through digital lending applications (DLA's). Listed herewith are suggestive key areas to focus during internal audit.

Regulatory Compliance:

- Ensure compliance with RBI (Reserve Bank of India) regulations, including NBFC guidelines.
- Verify adherence to the IT Act and data protection laws (e.g., GDPR, if applicable).
- Confirm compliance with the Fair Practices Code and grievance redressal mechanisms.

Loan Origination and Underwriting:

- Audit the process of customer onboarding, KYC (Know Your Customer), and underwriting standards.
- Evaluate credit risk assessment procedures and loan approval processes.
- Verify the accuracy and completeness of borrower documentation.

Risk Management:

- Assess the company's risk management policies and procedures.
- Examine credit risk, operational risk, and market risk assessment and mitigation strategies.
- Evaluate the adequacy of provisions for loan losses.

Data Security and Privacy:

- Review data security measures and privacy policies to protect customer information.
- Ensure data encryption, secure storage, and secure transmission of sensitive information.
- Verify compliance with GDPR or other applicable data protection laws.

Lending Platform Technology:

- Assess the reliability and security of the digital lending platform.

- Check for vulnerabilities, cyber threat mitigation, and disaster recovery plans.
- Evaluate the scalability and performance of the platform.

Customer Service and Complaint Handling:

- Audit customer service processes and response times.
- Ensure timely resolution of customer complaints and grievances.
- Review the feedback and rating systems in mobile applications.

Transaction Monitoring and Reporting:

- Evaluate the monitoring of transactions for suspicious activities or fraud.
- Ensure adherence to anti-money laundering (AML) and counter-terrorist financing (CTF) regulations.
- Review reporting mechanisms to regulatory authorities.

Third-Party Agreements:

- Examine agreements with lending service providers for transparency and compliance.
- Verify that contracts outline responsibilities, data-sharing, and service-level agreements.

Continuous Monitoring: Ensure company has established ongoing monitoring processes to ensure compliance and risk management.

Chapter 4
Understanding Risk

Types of Risks

4.1 Risks as faced by Non-Banking Financial Companies are as follows:

Credit Risk In the context of Non-Banking Financial Companies (NBFCs) in India, credit risk refers to the risk of borrowers defaulting on their loan repayments.	**Default Risk:** This is the risk that borrowers may fail to make their scheduled loan repayments. **Risk Mitigation**: Conduct thorough credit assessments and due diligence before extending loans. Diversify the loan portfolio to spread risk. Monitor borrower performance regularly and have a well-defined process for managing delinquent accounts.
	Credit Underwriting Risk: Poor credit underwriting practices can lead to higher default rates. **Risk Mitigation**: Implement robust underwriting standards, including the evaluation of borrower creditworthiness, income, and repayment capacity. Regularly review and update underwriting guidelines.
	Concentration Risk: This occurs when a significant portion of the loan portfolio is concentrated in a specific industry or with a few large borrowers. **Risk Mitigation**: Diversify the loan portfolio across different sectors and borrower types to reduce concentration risk. Set limits on exposure to single borrowers or groups of related borrowers.

Market Risk Market risk is the possibility that an individual or other entity will experience	**Asset Price Risk:** Changes in the market value of assets held by NBFCs, such as securities or real estate, can impact their financial position. **Mitigation:** Diversify the investment portfolio across asset classes and maturities. Regularly assess and

losses due to factors that affect the overall performance of investments in the financial markets. Non-Banking Financial Companies (NBFCs) in India are exposed to various market risks that can impact their financial stability and profitability.	adjust the portfolio based on market conditions.
	Currency Exchange Rate Risk: If an NBFC deals in foreign currencies or holds assets denominated in foreign currencies, fluctuations in exchange rates can lead to gains or losses. **Mitigation:** Hedge currency risk using financial derivatives like forward contracts or options. Maintain a natural hedge by matching foreign currency assets and liabilities.
	Market Liquidity Risk: Difficulty in selling assets or obtaining funding at favourable terms due to market illiquidity. **Mitigation:** Maintain an adequate liquidity buffer and access to various funding sources. Regularly stress-test the liquidity position
	Credit Spread Risk: Changes in credit spreads can impact the market value of debt securities in the investment portfolio. **Mitigation:** Diversify the credit risk in the investment portfolio. Monitor and adjust holdings based on credit quality and spreads.
	Commodity Price Risk: If the NBFC has exposure to commodities, fluctuations in commodity prices can impact profitability. **Mitigation:** Hedge commodity price risk using derivatives or reduce exposure to volatile commodities.
	Market Volatility Risk: Sudden market volatility can lead to price fluctuations in securities and investments. **Mitigation:** Implement risk management tools like stop-loss orders and limit orders. Diversify investments to reduce concentration risk.
	Systemic Risk: Events such as economic crises or

	market crashes can have a widespread impact on the financial system and NBFCs. **Mitigation:** Diversify the portfolio and maintain a strong capital base to withstand systemic shocks. Monitor systemic risk indicators and prepare contingency plans.
Note: Mitigating market risks requires a combination of risk management strategies, including diversification, hedging, stress testing, and active monitoring of market conditions. Additionally, a robust risk management framework and compliance with regulatory guidelines are essential for NBFCs to navigate market risks effectively.	

Liquidity Risk Liquidity risk refers to the risk that an NBFC (Non-Banking Financial Company) in India may not have access to sufficient funds to meet its short-term financial obligations when they come due.	**Funding Liquidity Risk**: Difficulty in obtaining funding from various sources, such as banks, financial markets, or depositors. **Mitigation**: Diversify funding sources, maintain a well-structured liability profile, and establish credit lines with banks. Develop relationships with multiple lenders to ensure access to funds.
	Asset Liquidity Risk: Difficulty in selling assets or loans at fair values in a distressed market. **Mitigation:** Ensure that assets held are relatively liquid or have secondary market outlets. Periodically assess the liquidity of the asset portfolio.
	Depositor Run Risk: Sudden withdrawal of deposits by depositors can lead to a liquidity crisis. **Mitigation:** Maintain strong customer relationships and communicate transparently with depositors. Have contingency plans and access to.
	Regulatory Liquidity Risk: Regulatory changes can impact liquidity requirements and affect an NBFC's ability to meet them. **Mitigation:** Stay abreast with regulatory changes and maintain a cushion of liquidity to meet any new

	regulatory requirements. Engage with regulatory authorities for guidance and compliance.
	Currency Liquidity Risk: Holding assets or liabilities denominated in foreign currencies can expose an NBFC to currency-related liquidity risk. **Mitigation**: Hedge currency risk using financial derivatives. Match foreign currency assets and liabilities to reduce exposure.
	Internal Liquidity Risk: Poor internal cash flow management and inadequate forecasting can lead to liquidity shortfalls. **Mitigation:** Implement robust cash flow forecasting mechanisms. Set up liquidity risk management committees to monitor and manage internal liquidity risks effectively.
	Counterparty Liquidity Risk: The inability of counterparties to meet their obligations can disrupt the NBFC's cash flows. **Mitigation:** Conduct due diligence on counterparties and counterparties' liquidity positions. Diversify counterparties to reduce concentration risk.
Note: To mitigate liquidity risks effectively, NBFCs should develop and implement a comprehensive liquidity risk management framework that includes stress testing, contingency planning, and access to backup funding sources. Regular monitoring and reporting of liquidity metrics are also crucial to maintaining financial stability.	

Regulatory or Compliance Risk Regulatory and compliance risks for Non-Banking Financial Companies (NBFCs) in India	**Regulatory Reporting and Filing Risk**: Failure to submit accurate and timely regulatory reports and filings, leading to penalties or regulatory actions. **Mitigation:** Establish a robust reporting framework with dedicated personnel responsible for compliance. Implement automated systems to ensure.
	Capital Adequacy Risk: Inadequate capitalization to meet regulatory capital adequacy requirements, which

arise from the complex and evolving regulatory environment. These risks can have legal, financial, and reputational implications.	can lead to restrictions on business operations. **Mitigation**: Conduct regular capital adequacy assessments and maintain capital buffers above regulatory minimums. Plan for capital infusion well in advance if needed.
	Compliance with Prudential Norms Non-compliance with prudential norms related to asset classification, provisioning, and income recognition. **Mitigation:** Develop comprehensive policies and procedures to ensure adherence to prudential norms. Conduct regular internal audits to identify and rectify compliance issues.
	Anti-Money Laundering (AML) and Know Your Customer (KYC) Risk: Inadequate AML and KYC procedures can expose an NBFC to money laundering activities and financial crime. **Mitigation**: Implement robust AML and KYC procedures, including customer due diligence and suspicious transaction monitoring. Train employees to recognize and report suspicious activities.
	Interest Rate Regulations: Non-compliance with interest rate regulations, such as caps on lending rates. **Mitigation**: Ensure that lending practices adhere to interest rate regulations and regularly review and adjust interest rates in line with regulatory guidelines.
	Data Privacy and Security Risk: Mishandling or unauthorized access to customer data can result in legal and reputational damage. **Mitigation:** Implement strong data privacy and security measures, including encryption and access controls. Comply with data protection laws and regulations.
	Fair Practices Code Violations: Failure to follow fair lending and debt recovery practices can lead to legal actions and reputational damage. **Mitigation**: Develop a Fair Practices Code that outlines ethical and fair lending practices. Train

	employees on these practices and regularly audit adherence.
	Corporate Governance Risk: Weak corporate governance practices can result in regulatory scrutiny and investor distrust. **Mitigation:** Establish a strong corporate governance framework with independent directors, transparent decision-making processes, and an effective board of directors.
	Compliance with NBFC Regulations: Non-compliance with specific NBFC regulations, such as capital requirements, asset classification norms, or priority sector lending targets. **Mitigation**: Stay abreast with NBFC regulations and making necessary adjustments to ensure compliance. Engaging with regulatory authorities for guidance on complex issues.
Note: To mitigate regulatory and compliance risks effectively, NBFCs should establish a compliance culture within the organization, conduct regular internal audits, and engage with legal and regulatory experts for guidance. It's essential to stay informed about changes in regulations and adapt proactively to remain compliant.	

Asset-Liability Mismatch Risk Asset-liability mismatch (ALM) risk occurs when the maturity and interest rate characteristics of an NBFC's assets and liabilities do not align, potentially leading to financial	**Maturity Mismatch Risk:** When the maturity of an NBFC's assets differs significantly from that of its liabilities, it can lead to difficulties in repaying creditors or taking advantage of profitable investment opportunities. **Mitigation:** Match the maturities of assets and liabilities as closely as possible. Use ALM modelling to identify and quantify maturity gaps and take corrective actions.
	Interest Rate Mismatch Risk: This occurs when the interest rates on assets and liabilities are not in sync. For example, if short-term liabilities are funded at variable rates while long-term assets yield fixed rates,

instability.	changes in interest rates can impact profitability. **Mitigation**: Regularly review and align the interest rate structures of assets and liabilities. Consider using interest rate swaps or other derivatives to manage interest rate risk.
	Currency Mismatch Risk: If an NBFC holds assets or liabilities denominated in foreign currencies, fluctuations in exchange rates can lead to losses if not managed properly. **Mitigation:** Hedge currency risk using financial derivatives, match foreign currency assets and liabilities where possible, or use natural hedging strategies to reduce exposure.
	Liquidity Mismatch Risk: Mismatch in the liquidity profiles of assets and liabilities can result in difficulties in meeting short-term obligations. **Mitigation**: Maintain an adequate liquidity buffer to cover potential short-term funding needs. Conduct regular stress tests to assess liquidity positions under various scenarios.
	Repricing Risk: When assets and liabilities reprice at different times or frequencies, changes in interest rates can affect profitability. **Mitigation:** Monitor and manage repricing risk by aligning the repricing intervals of assets and liabilities. Diversify funding sources to reduce reliance on short-term borrowings.
Note: Mitigating ALM risks requires a combination of strategies, including regular ALM modelling and monitoring, diversification of assets and liabilities, and the use of financial derivatives to manage interest rate and currency risks. Developing a comprehensive ALM policy and adhering to regulatory guidelines is essential for effective risk management in NBFCs.	

Credit Concentration Risk	**Industry Concentration Risk:** When a substantial portion of an NBFC's loan portfolio is invested in a particular industry or sector, adverse developments in that industry (e.g., economic downturn or regulatory

Credit concentration risk in Non-Banking Financial Companies (NBFCs) in India occurs when a significant portion of the loan portfolio is concentrated in a specific industry, sector, or with a few large borrowers. Here are types of credit concentration risks and risk mitigation strategies:	changes) can lead to higher default rates. **Mitigation:** Diversify the loan portfolio across various industries and sectors to reduce industry concentration. Set limits on exposure to specific sectors and regularly assess industry-specific risks.
	Borrower Concentration Risk: Overreliance on a few large borrowers or group entities can expose the NBFC to significant credit risk if these borrowers face financial difficulties. **Mitigation:** Implement concentration limits on exposure to single borrowers or related groups. Regularly monitor the creditworthiness of large borrowers and adjust lending strategies accordingly.
	Geographic Concentration Risk: f an NBFC primarily operates in a specific geographic region, it can be vulnerable to local economic shocks or regional crises. **Mitigation:** Diversify operations and lending activities across multiple geographic regions. Assess and manage regional economic risks as part of the credit risk management process.
	Product Concentration Risk: Concentration in specific loan products or categories can expose an NBFC to risks associated with those products, such as changes in regulatory treatment or market demand. **Mitigation:** Diversify the loan product portfolio to spread risk. Continuously monitor changes in market conditions and regulations affecting specific products.
	Counterparty Concentration Risk: For NBFCs involved in trading or derivative activities, concentration in a few counterparties can lead to significant credit exposure. **Mitigation**: Set counterparty exposure limits and regularly review and adjust these limits. Diversify counterparties and monitor their creditworthiness.
	Size Concentration Risk: Overconcentration of loans to either small or large borrowers can increase credit

	risk. Small borrowers may have higher default rates, while large borrowers can create significant exposure. **Mitigation:** Maintain a balanced mix of small, medium, and large borrowers in the loan portfolio. Implement risk-based lending criteria to assess creditworthiness.
	Product Type Concentration Risk: Focusing on a specific type of lending product (e.g., personal loans, vehicle loans) can expose an NBFC to the risks associated with that product category. **Mitigation:** Diversify the lending product portfolio and regularly assess the risk profiles of different product types. Adjust lending strategies based on changing risk assessments.

Cybersecurity Risk Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. Cybersecurity risks are a significant	**Data Breaches:** Unauthorized access or theft of customer data, including personal and financial information. **Mitigation:** Implement robust data encryption, access controls, and intrusion detection systems. Conduct regular security audits and penetration testing.
	Phishing and Social Engineering: Cybercriminals trick employees or customers into revealing sensitive information or conducting fraudulent transactions. **Mitigation:** Educate employees and customers about phishing risks. Implement email filtering and multi-factor authentication.
	Ransomware Attacks: Malicious software can encrypt critical data and demand a ransom for decryption. **Mitigation:** Maintain up-to-date antivirus and anti-malware solutions. Regularly back up data and establish an incident response plan.
	Insider Threats: Employees or contractors with

concern for Non-Banking Financial Companies (NBFCs) in India, as they handle sensitive financial data and transactions.	malicious intent or unintentional negligence can compromise security. **Mitigation:** Implement role-based access controls, monitor employee activities, and conduct security awareness training.
	Third-Party Vendor Risks: Vulnerabilities in third-party systems or services can expose NBFCs to cyber risks. **Mitigation:** Assess third-party security practices and require vendors to meet cybersecurity standards. Include security clauses in vendor contracts.
	Mobile App Vulnerabilities: Mobile apps used by customers may have security vulnerabilities, leading to data breaches or fraud. **Mitigation:** Regularly update and patch mobile apps. Implement app security testing and code reviews.
	Denial of Service (DoS) Attacks: Attackers overwhelm NBFC systems with traffic, rendering services unavailable. **Mitigation:** Use traffic filtering and load balancing solutions to mitigate DoS attacks. Have a disaster recovery plan in place

Note: Mitigating Cybersecurity risks is an ongoing process that requires vigilance, regular assessment, and adaptation to evolving threats. Collaboration with cybersecurity experts and threat intelligence sharing can also enhance NBFC cybersecurity defences. Other Risk Mitigation Strategies:

Cybersecurity Policies and Training: Develop and enforce comprehensive cybersecurity policies. Provide regular training to employees and customers on cybersecurity best practices.

Network Security: Implement firewalls, intrusion detection systems, and intrusion prevention systems to protect against unauthorized access and malware.

Data Encryption: Encrypt sensitive data both in transit and at rest to protect it from interception or theft.

Incident Response Plan: Establish an incident response plan that outlines steps to take in case of a cybersecurity breach. Test and update this plan regularly.

Patch Management: Keep all software, operating systems, and applications up-to-date with security patches.

Vendor Due Diligence: Conduct thorough cybersecurity assessments of third-party vendors and partners.

Multi-Factor Authentication (MFA): Implement MFA for access to critical systems and sensitive data.

Regular Audits and Testing: Conduct cybersecurity audits, vulnerability assessments, and penetration testing to identify and address weaknesses.

Backup and Recovery: Regularly back up critical data and ensure a robust disaster recovery plan is in place.

Regulatory Compliance: Stay updated on cybersecurity regulations in India and comply with relevant standards and guidelines.

Reputational Risk Reputational risk in financial services is associated with an institution losing consumer or stakeholder trust. It's the risk that those consumers and stakeholders will take on a negative perception of the institution– whether it's one branch or the entire brand – following a particular event. This risk is a significant concern for Non-Banking Financial Companies	**Operational Failures:** Poor operational practices, including data breaches, system outages, or service disruptions, can damage the reputation of an NBFC. **Mitigation**: Implement robust cybersecurity measures, disaster recovery plans, and conduct regular system audits.
	Mismanagement and Fraud: Mismanagement of funds, financial irregularities, or involvement in fraudulent activities can lead to reputational damage. **Mitigation:** Maintain strong internal controls, governance, and compliance practices. Conduct thorough background checks on employees and partners.
	Compliance and Regulatory Violations: Non-compliance with financial regulations, customer protection laws, or unethical conduct can harm an NBFC's reputation. **Mitigation:** Stay abreast with regulatory

(NBFCs) in India, as it can affect trust, credibility, and the ability to attract and retain customers and investors.	requirements, maintain a robust compliance management system, and conduct internal audits.
	Customer Complaints and Disputes: Unresolved customer complaints or disputes can escalate, leading to reputational harm. **Mitigation:** Implement effective complaint resolution mechanisms, address customer concerns promptly, and prioritize customer satisfaction.
	Negative Media Coverage: Adverse media reports, whether accurate or not, can quickly tarnish an NBFC's reputation. **Mitigation**: Develop a crisis communication plan to respond to negative media coverage promptly. Focus on transparency and proactive communication.
	Market Rumours and Speculation: Rumours and speculation can lead to market panic and loss of confidence in the NBFC. **Mitigation:** Actively monitor and address market rumours. Provide accurate and timely information to stakeholders.

Note: Reputation risk management should be an integral part of an NBFC's overall risk management framework. It requires vigilance, proactive measures, and a commitment to maintaining trust and credibility in the financial market.

Other Risk Mitigation Strategies:

Ethical Business Practices: Maintain the highest ethical standards in all business activities and decisions.

Strong Corporate Governance: Ensure a transparent and accountable corporate governance structure.

Regulatory Compliance: Comply with all applicable financial regulations and customer protection laws.

Customer-Centric Approach: Prioritize customer satisfaction, responsiveness to complaints, and transparent communication.

Crisis Management: Develop a crisis management plan that includes communication strategies and action plans for reputational threats.

Reputation Monitoring: Continuously monitor online and offline channels for any negative mentions or rumours related to the NBFC's reputation. **Social Responsibility**: Engage in corporate social responsibility (CSR) initiatives to demonstrate commitment to societal well-being. **Stakeholder Engagement**: Build and maintain strong relationships with customers, investors, regulators, and the media. **Employee Training**: Train employees on ethical conduct, compliance, and the importance of safeguarding the company's reputation. **Transparency:** Be transparent in financial reporting, disclosures, and communication with stakeholders.

Environmental and Social Risk (ESG Risks) These Risks are increasingly important considerations for Non-Banking Financial Companies (NBFCs) in India as they impact long-term sustainability and reputation.	**Environmental Impact Risk:** NBFCs may inadvertently finance projects or activities with adverse environmental impacts, such as deforestation or pollution. **Mitigation**: Develop and enforce environmental and social risk assessment processes for lending and investment decisions. Set clear environmental criteria for project financing.
	Social Impact Risk: Financing projects or businesses that have negative social impacts, such as labour rights violations or community displacement. **Mitigation**: Conduct due diligence on borrowers and investees to assess their social impacts. Implement responsible lending and investment principles.
	Reputation Risk: Negative publicity or stakeholder backlash due to perceived environmental or social misconduct can damage the reputation of an NBFC. **Mitigation:** Develop and communicate clear ESG policies and practices. Actively engage with stakeholders, be transparent about ESG efforts, and address any issues promptly.
	Regulatory and Legal Risks: Non-compliance with evolving ESG regulations and disclosure

	requirements can result in legal actions and penalties. **Mitigation:** Stay informed about ESG regulations and ensure compliance. Establish a dedicated ESG compliance function if necessary.

Note: Mitigating ESG risks requires a holistic approach that involves embedding ESG considerations into the organization's culture, operations, and decision-making processes. This not only helps manage risks but also positions NBFCs for long-term sustainability and resilience in a changing global landscape.

Other Risk Mitigation Strategies:

ESG Integration: Integrate ESG factors into the credit assessment process, considering the environmental and social impacts of borrowers' activities.

Environmental and Social Due Diligence: Conduct thorough due diligence on potential borrowers, including assessing their environmental and social risk profile.

Stakeholder Engagement: Engage with stakeholders, including customers, investors, and communities, to understand their ESG concerns and expectations.

Responsible Lending and Investment: Develop lending and investment criteria that prioritize sustainable and socially responsible projects and businesses.

ESG Reporting and Disclosure: Publish ESG reports and disclosures, including efforts to reduce carbon emissions and social impact assessments.

Sustainable Finance Products: Offer sustainable finance products that promote environmental and social responsibility.

ESG Training: Provide ESG training to employees to ensure they understand the importance of ESG risk management.

ESG Governance: Establish an ESG committee or department responsible for overseeing and implementing ESG policies and initiatives.

Collaboration: Collaborate with industry peers, ESG experts, and regulatory bodies to share best practices and stay updated on ESG trends and requirements.

Outsourcing or Third-party Risk Outsourcing or third-party risks are significant considerations for Non-Banking Financial Companies (NBFCs) in India, as they often rely on external service providers to support various functions.	**Disruptions or failures in third-party operations**: Disruptions or failures in third-party operations can impact the NBFC's operations, leading to service disruptions, data breaches, or compliance issues. **Mitigation:** Conduct thorough due diligence on third-party service providers, including their operational and cybersecurity capabilities. Establish clear service level agreements (SLAs) and contingency plans for service disruptions.
	Data Security and Privacy Risk: Third-party providers may have access to sensitive customer data, leading to data breaches or non-compliance with data protection regulations. **Mitigation:** Implement strong data security measures, including encryption and access controls. Ensure that third-party contracts include data protection clauses and audit rights.
	Compliance and Regulatory Risk: Non-compliance by third-party providers with relevant regulations can expose the NBFC to regulatory scrutiny and penalties. **Mitigation:** Conduct regular audits of third-party compliance with applicable regulations. Include regulatory compliance requirements in contracts.
	Reputation Risk: Third-party actions or misconduct can reflect poorly on the NBFC's reputation. **Mitigation:** Choose third-party providers with strong ethical practices and reputations. Maintain transparency and clear communication with customers regarding third-party relationships.
	Vendor Concentration Risk: Overreliance on a single third-party provider for critical functions can increase vulnerability to disruptions. **Mitigation:** Diversify third-party relationships for critical functions to reduce vendor concentration risk. Develop alternative sourcing strategies.

Enterprise Risk Management (ERM*) vs* Operational Risk Management (ORM)

4.2 The Enterprise-wide risk management is a concept in which the management of risks is integrated and coordinated across the entire organization and a culture of risk awareness is created. Companies across a wide cross-section of industries are beginning to implement this effective new methodology.

Operational risk management (ORM) is a subset of ERM that focuses on identifying, analysing, monitoring, and controlling operational risk.

At first glimpse, there is much similarity between operational risk management and other classes of risk (e.g., credit, market, liquidity risk, etc.) and the tools and techniques applied to them. In fact, the principles applied are nearly identical. Both ORM and ERM must identify, measure, mitigate and monitor risk. However, at a more detailed level, there are numerous differences, ranging from the risk classes themselves to the skills needed to work with operational risk.

In essence, whilst ERM is proactive, ORM is protective. Enterprise Risk Management (ERM), emphasize optimizing risk appetites to balance risk-taking and potential rewards, ORM processes primarily focus on controls to minimise or eliminate operational risk.

Management of ERM in an Organization

The Board of Directors and executive management are both in charge of determining what ERM process should be in place as well as how ERM across the organization should function. More specifically, an organization's top management is responsible for designing and implementing the ERM process, while the Board of Directors is responsible for providing oversight. This oversight includes the understanding and approval of ERM processes and overseeing identified risks to ensure responses are within the stakeholders' risk appetite.

Role of Board of Directors/ Governing Body

The board should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective enterprise risk management.

The board should consider seeking input from internal auditors, external auditors, and Others. Responsibilities of the board and management on ERM are clearly stated in the international frameworks (such as the ERM Framework) and the Corporate Governance Code. Generally, the board should oversee the ERM by:

- Define expectations;
- Set strategy & high-level objectives;
- Resource allocation;
- Adopt risk management policy;
- Knowing the extent of ERM within the organization;
- Reviewing the risk portfolio of the organization and considering it against the risk appetite;
- Understanding the changes and significant risks the organization is facing; and
- Considering whether the risk responses are appropriate or not.

Understanding Risk Appetite and Risk Tolerance

Risk appetite is the amount of risk an organization or investor is willing to take in pursuit of objectives it deems have value. Risk appetite can also be described as an organization's risk taking capacity, or the maximum amount of residual risk it will accept after controls and other measures have been put in place. Risk tolerance, by contrast, is the amount of deviation from its risk appetite that an organization is willing to accept to achieve a specific objective, based on parameters that include industry and vertical standards.

A Chief Risk Officer (CRO) role is responsible to manage overall ERM. The CRO is in charge of identifying, analysing and mitigating risks that impact the organization as a whole. The CRO also ensures that an organization complies with any government regulations and reviews factors that could hurt investments or a company's business units.

Roles and Responsibilities of Internal Auditor

ICAI has issued Standard on Internal Audit (SIA) 130, Risk Management. This Standard seeks to clarify the concept and also the responsibility of the Internal Auditor, Management and other Stakeholders with respect to risk management, keeping in mind the legal, regulatory and professional obligations. This Standard applies to all risk based internal audits and also

where risk management framework is a subject matter of an audit, and is being assessed, evaluated and reported upon.

The purpose of this Standard on Risk Management is to:

(a) Provide a common terminology by defining various risk management terms to prevent ambiguity and provide clarity on the subject matter;

(b) Explain the responsibilities of the Board of Directors, risk management department and management with regard to risk management, as mandated by law and regulations; and

(c) State the responsibilities of the internal auditor, especially when providing an assurance on the risk management framework.

Fraud Risks and Specific Challenges

4.3 "Fraud" is a deliberate wrong or criminal act with an intent to deceive another whether or not there is a financial gain at the cost of any person or entity/ organisation. It is essential for NBFC, being an organisation for managing its risk, to ensure that its employees are aware of what constitutes a fraud, how they should avoid such acts, stay alert and bring to the notice of the management any deviations that can be construed as fraudulent to the appropriate authority. The management needs to ensure that systems have in-built mechanisms to detect frauds. Once detected, it is ensured that measures to gather evidence against the perpetrators of the fraud are established.

Fraud Detection and Fraud Deterrence

Each organization has its own established value systems and, therefore, would like its employees to follow a code of conduct. This provides the management a medium to interact with employees in defining the ground rules to be followed and actions that are acceptable or not acceptable. For the purpose, management must define what types of conduct may involve conflict of interest (or potential for a conflict of interest) vis- à-vis the official duties. This may or may not involve any pecuniary interest and may extend to any bias towards third persons in the official dealings/ decisions. Hence, non-competitive pricing of products or unjustified commercial dealings could be within the purview of this code of conduct.

Generally, employees are the first point of contact in noticing a fraudulent activity arising out of any unusual or abnormal practices. These may remain

unreported to the superior officers due to lack of training and awareness among the employees. The insecurity among employees is another reason for not escalating the matter to the superior authority. Therefore, employees need to be made aware of their role in detection as well as deterrence to such fraudulent acts and appreciate the reporting process through established procedures.

Apart from providing abundant opportunity to the employees within the organization to stay away from fraudulent acts and to report any such deceit to the appropriate authority, it is essential to set up independent monitoring system or devise strategies which work coherently with the following objectives:

- Identification and reporting of unusual activities;
- Isolating deviations and surveillance mechanism in the day- to-day operations;
- Use of computer applications and audit tools in keeping track of unusual transactions;
- A robust accounting and management information reporting system; and
- Effective interaction with the Chief Internal Auditor for appropriate audit reviews.

It is preferable that there should be an effective incident reporting process normally to a designated official (heading the investigative cell or compliance officer) to whom all the suspected activities will be reported. It should be his responsibility to promptly update the management of such incident.

The senior management executives need to consistently make an effort of educating the employees and related third parties on how to be alert to fraudulent activities, including suspicious activities and the manner in which the same needs to be communicated. In addition, the internal audit observations can be filtered to identify red flags and used as a medium to apprise employees of internal control gaps in prevention or detection of frauds.

When a fraud is suspected, certain immediate steps may need to be taken to prevent loss of evidence or furtherance of such acts. For the purpose, records and documents are taken in safe custody and the persons connected with the activities are generally transferred to other activities till the perpetrator of the fraud is identified. The scope and period of coverage is

dependent on judgement and this in turn would determine the time required to complete the assessment process.

These may relate more to the activities impacted due to fraud including fraudsters' access to records, documents, and information. Unravelling the modus operandi of the fraudulent act could be equally complex with reference to identifying and deciphering the trail left by the fraudster and in gathering requisite evidence. This is followed by an assessment of damages arising out of the wrongful act. In case the entity has an insurance cover, the insurer is informed of the incident and thereafter the extent of damages is notified. The management has the option of either proceeding with legal action or can take disciplinary action on the erring employee or third party if the situation warrants. Where the perpetrator is not known steps may be taken for in-depth investigation either by in- house resource or external agencies.

Initiating Investigative Process

Once a fraud is reported, a preliminary investigation to be conducted first to assess and verify the enormity of the act and then the next step is to substantiate it with evidence. It is preferred that this is carried out under the aegis of, generally, a Chief Financial Officer in full time employment with the company.

The Fraud Risk Officer, generally, a person of integrity and based on his past track record, have the ability to manage situations of fraud risk. He is, normally, a person who is trusted by the management in safeguarding the reputation and image of the organization.

To achieve this objective, a Fraud Risk Officer is an official who by the nature of his duties, generally, reports to the senior most officer in the company (Chief Risk officer or CEO/ Managing Director). The Fraud Risk Officer may seek the support of the internal auditor in discharging his duties on matters relating to the investigation.

Fraud Risk Officer assists the management in conducting the preliminary assessment of each situation and depending upon the magnitude of suspected fraud (which is by and large a matter of subjective judgment) will decide whether they have the resources within the organization to carry out a full-fledged investigation and the extent of outsourcing of the investigative activities.

Fraud Risk Officer role and responsibility may include the following:

a) Interaction with the internal auditor of the company.

b) Resource mobilization, either internally or outsourced for conducting investigation.

c) Sequencing of the events and activities for diagnosis of the problem.

d) Internal control assessment in highlighting vulnerabilities.

e) Preliminary assessment on the role of internal and external persons who are suspected to be involved in the alleged irregularities and details thereof.

f) Damage assessment arising out of the reported incident.

g) Collation of information on suspected fraudulent activity.

h) Ensuring a reporting format to the senior management or regulators such as RBI, IRDA, SEBI, NHB, etc.

i) Comment on available evidence to form an opinion.

Considering the sensitivities involved in any information that relates to a fraudulent activity, it is essential that adequate confidentiality is ensured in collating such information and reporting. Based on his report, management can form an opinion on the future course of action including referral for legal action, reporting to police authorities, filing of insurance claims, disciplinary action against delinquent employees, etc.

Managing Risk

The role of a Fraud Risk Officer / investigating person/authority is different from that of the line functionaries, as his primary concern would be to corroborate facts based on available evidence, within the legal realms. Senior executives must give a free hand to the investigating officer and should not intrude into their investigative approach and methodology. Such intrusion tends to be counterproductive. The desired course of management action will depend on the regular updates on the progress made in the investigation. It may be noted that just as the senior management is responsible for initiating the investigation, they have a similar right to call off an investigation.

Post discovery of a fraudulent activity, the manner in which the enquiry process is conducted may be defined through a policy document. This will include the options available for disciplinary actions that could be explored by the management.

Anti-fraud programs enable the management to identify areas that are vulnerable to potentially fraudulent activities. Where such events are inherent to the business environment, counter measures for identification of irregularities and timely action should be ensured.

Unless warranted by law or regulatory institutions such as, Reserve Bank of India norms, it is the management's discretion as to whether an incident needs to be reported to the police authorities. A weak or inadmissible evidence or reputation risk to the organization is sometimes a reason for not proceeding legally against the erring employees.

The management to ensure that the above incidents are brought to the notice of the Chief Internal Auditor in a timely manner, including management action plan and corrective steps, to be taken post discovery of the fraud. There should be a standard format in which the management informs the audit committee and the board about the status of frauds reported, persons involved, types of fraud, recoveries, corrective measures, and regular updates on investigations in progress.

Responsibilities and Roles for Prevention and Detection of Frauds

The primary responsibility for prevention and detection of frauds is that of the management of the entity. The internal auditor should, however, help the management fulfil its responsibilities relating to fraud prevention and detection. Thus, accountability on detection of fraud is with the management and they may engage the services of internal auditors as facilitators. Similarly, the role of statutory auditors on matters relating to reporting on fraudulent is defined under Standard on Auditing (SA) 240 "The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements".

Role of Management

Standard on Internal Audit (SIA) 11, "Consideration of Fraud in an Internal Audit" provides that:

The *control environment* sets the tone at the top in an entity and greatly impacts the effectiveness of internal controls. It includes the following:

- The policies and procedures established by the management to communicate and enforce the culture of integrity and ethical values in the entity.
- Management's commitment to competence.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resources policies and practices.

The entity's risk assessment process includes the policies and procedures adopted by the management to identify risks that can affect the achievement of the objectives of the entity and to distinguish risks from opportunities. In the context of prevention of frauds, the entity's risk assessment process would include the policies and procedures of the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets.

The information system and communication refer to the policies and procedures established by the management to identify, capture, and communicate relevant information to the concerned persons in the entity to enable them to make timely and effective decisions and discharge their responsibilities efficiently. In the context of frauds, such policies and procedures could take form of whistle-blower policies and mechanisms, ethics help lines and counselling, training of employees, etc.

The control activities refer to the policies and procedures established by the management to ensure that the risks identified are responded to as per the policy or the specific decision of the management. In the context of frauds, the control activities include actions taken by management to prevent or detect and correct the frauds or breach of internal controls.

Monitoring refers to continuous supervision and assessment of the internal controls to identify instances of any actual or possible breaches therein and to take corrective action on a timely basis.

Role of Internal Audit

Standard on Internal Audit (SIA) 11, Consideration of Fraud in an Internal Audit as issued by ICAI provides guidance on the designing and implementation of the internal controls in an entity that would also help the internal audit to assess the risk of frauds. The Standards also establishes the

responsibilities of the internal auditor relating to the fraud prevention and detection.

The SIA also provide guidance regarding the communication and documentation of fraud.

Basic Principles Governing Internal Audit- An internal auditor should use his knowledge and skills to enable him to reasonably identify indicators of frauds. Although, normally, an internal auditor is not expected to possess skills and knowledge of a person expert in detecting and investigating frauds, he should, however, have reasonable knowledge of factors that might increase the risk of opportunities for frauds in an entity and exercise reasonable care and professional scepticism while carrying out internal audit.

Responsibilities of the Internal Auditor - The internal auditor should, help the management fulfil its responsibilities relating to fraud prevention and detection.

- **Control environment -** The internal auditor should obtain an understanding of the various aspects of the control environment and evaluate the same as to the operating effectiveness.
- **Risk Assessment** - The internal auditor should obtain an understanding of the policies and procedures adopted by the management to identify risks that can affect the achievement of the objectives of the entity and to distinguish risks from opportunities and evaluate the effectiveness of these policies and procedures. In the context of prevention of frauds, the internal auditor should specifically evaluate the policies and procedures established by the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets.
- **Information system and communication** - The internal auditor should assess the operating effectiveness of the policies and procedures established by the management to identify, capture and communicate relevant information to the concerned persons in the entity to enable them to make timely and effective decisions and discharge their responsibilities efficiently. The internal auditor should assess whether the controls implemented by the management to ensure that the risks identified are responded to as per the policy or the specific decision of the management, as the case may be, are in fact working effectively and whether they are effective in prevention or

timely detection and correction of the frauds or breach of internal controls.

- **Monitoring** - The internal auditor should evaluate the mechanism in place for supervision and assessment of the internal controls to identify instances of any actual or possible breaches therein and to take corrective action on a timely basis.
- **Communication of Fraud** - The internal auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for his findings contained in his report and suggest remedial action. However, in case the internal auditor comes across any actual or suspected fraud or any other misappropriation of assets, he should immediately bring the same to the attention of the management.
- **Documentation:** The internal auditor should document fraud risk factors identified as being present during the internal auditor's assessment process and document the internal auditor's response to any other factors. If during the performance of the internal audit fraud risk factors are identified that cause the internal auditor to believe that additional internal audit procedures are necessary, the internal auditor should document the same.

Regulatory Requirements RBI has issued a Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016 made applicable to all deposit taking non-banking financial companies and 'systemically important non-deposit taking non-banking financial companies' (NBFC-ND-SI2) hereinafter called as 'Applicable NBFCs'.

Third Party Risk Management (TPRM)

Third Party Risk Management is a comprehensive framework and set of practices that organizations, particularly in the financial industry, use to identify, assess, monitor, and mitigate risks associated with their relationships with third-party entities, such as vendors, suppliers, service providers, and outsourcing partners. TPRM is a critical component of operational risk management and compliance in many industries, including banking, insurance, healthcare, real estate, etc.

Various suppliers can become third parties once introduced into the supply chain, including software and general service providers. Each third party can

introduce different security, privacy, business continuity, business reputation, and regulatory compliance risks.

A third-party risk assessment involves analyzing the risks introduced by third-party relationships along the organization's supply chain. It is a critical part of every third-party risk management program, providing the information needed to create a program suitable to the organization's specific risks, standards, and compliance requirements.

Applying proper risk management is critical for modern, interconnected organizations because these relationships create entry points for attackers. However, not every third party requires the same level of risk management and attention. Risk levels and impact vary between third-parties, and organizations need to classify vendors by access and risk levels,

Third parties that do not have access to confidential information or computer networks pose lesser risk than parties that offer more interconnected services. An office supplies vendor, for example, does not pose the same level of risk as a Software as a Service (SaaS) provider processing customer payments.

Though NBFCs do not have specific guidelines related to TPRM, however, Outsourcing guidelines issued by RBI captures vital elements required to manage risks related to third parties.

TPRM includes a focus on ensuring that third-party relationships adhere to regulatory requirements. It involves assessing whether third-party providers are compliant with relevant laws and regulations in the jurisdictions where they operate and serve their clients.

TPRM, as a broader concept, encompasses the risk management of all third-party relationships, not just outsourcing. It includes identifying, assessing, and managing various risks, such as operational, financial, strategic, and compliance risks, associated with third-party relationships.

Financial institutions must conduct due diligence to assess the suitability and reliability of third-party providers before entering into agreements or renewing contracts.

Operational resilience is a broader concept within TPRM. It involves evaluating and enhancing the resilience of an institution's operations in the face of disruptions or incidents related to third-party services, IT systems, or other critical dependencies.

Governance and oversight are core components of TPRM. It includes establishing roles and responsibilities, defining reporting structures, and implementing ongoing monitoring of third-party relationships.

TPRM provides a more comprehensive approach to managing third-party relationships across an institution's entire ecosystem. It's important for financial institutions to integrate the RBI's outsourcing guidelines into their overall TPRM framework to ensure comprehensive risk management and compliance with regulatory requirements.

Emerging Risks

4.4 Financial Services industry is most hit from risk perspective and it always faces challenges of new emerging risks. Some of the important emerging risks and how an NBFC can prepare themselves better for mitigating those risks:

Technology Risks

Cyber Security

Cybersecurity has emerged as a significant and rapidly evolving risk in the financial industry, affecting a wide range of institutions, including Non-Banking Financial Companies (NBFCs). As technology advancements continue to transform the financial landscape, the risk landscape has also shifted, with cyber threats posing an ever-increasing challenge.

Cybersecurity refers to the practices, technologies, and strategies implemented to protect computer systems, networks, and data from unauthorized access, cyberattacks, and data breaches. With the increasing digitization of financial services, the risk associated with cybersecurity has grown exponentially.

As per Sentinel One report, As of December 2022, finance and insurance organizations globally experienced 566 breaches, leading to over 254 million leaked records.

Ransomware attacks on financial services have increased from 55% in 2022 to 64% in 2023, which is nearly double the 34% reported in 2021. Only 1 in 10 attacks were stopped before encryption took place, making a total of 81% of organizations a victim of data encryption.

Data breaches cost the finance sector the second highest costs amongst all others at $5.9 million.

To mitigate the cyber security risks, an NBFC must:

- Implement a comprehensive cybersecurity framework, including firewalls, intrusion detection systems, and encryption, to protect against cyber threats.
- Train employees on cybersecurity best practices to minimize the risk of human error leading to breaches.
- Develop an incident response plan to contain and mitigate the impact of breaches, including communication with affected parties.
- Stay abreast of regulatory guidelines and ensure compliance to avoid legal and financial repercussions.
- Continuously monitor networks and systems for signs of intrusion and implement threat intelligence to proactively identify potential risks.
- The emergence of cybersecurity as an increasingly prominent risk highlights the need for NBFCs to adopt a proactive approach to protect their customers, operations, and reputation. As financial services continue to evolve in the digital age, the importance of robust cybersecurity measures cannot be overstated. Cybersecurity is no longer an option but an imperative for the continued success and sustainability of NBFCs.

Fintech

The rise of financial technology, or fintech, is transforming the financial services landscape, offering innovative solutions and challenging traditional banking and NBFCs. While fintech offers numerous opportunities, it also presents emerging risks that NBFCs must navigate.

Fintech is the application of technology to deliver financial services, including mobile payments, peer-to-peer lending, AI-advisors, and blockchain-based solutions.

Fintech industry is one of the fastest growing in the world. Using tech innovation, companies are helping traditional banks and NBFCs to grow and compete better. Like with any emerging industry, there are risks and opportunities.

Major Risks and Challenges Faced by Fintech

At present like majority of the start-ups, majority of Fin Techs are undercapitalized and inefficient with weak business models and high spending. These might not be able to survive in long run. Accordingly, there is a need to ascertain the impact of FinTech on financial stability, due to

higher potential for system-wide risk with its expansion. Lending standards could weaken due to wider credit access and higher competition. Reputational, cyber and third-party risks may arise for NBFCs interacting with FinTechs.

Fintechs face more challenges on data use, protection and privacy than other businesses. Due to an over-reliance on cutting-edge tech and the processing of sensitive financial data, fintech is often targeted for cyberattacks. While tech can help them scale, it can also be a source of disruptions and outages.

As the Indian population becomes data-rich with increasing Internet and mobile coverage, the next challenge is empowering consumers with the data generated by them through adequate legal and regulatory interventions. Citizens should be able to exercise control of their data like any other personal asset. There is an emerging demand for data localisation from various jurisdictions.

Outages/downtime can lead to lost business if customers can't access services. Fintech firms are more likely to be targeted than traditional financial institutions. For example, if a fintech company falls victim to a data breach and customer data is compromised, the reputational damage and loss of user trust are disastrous for businesses.

Access to Fin Tech is still limited – majorly in urban areas. Rural areas where most of India's population resides, still finds it difficult to access these solutions creating an inequality of access to Fin Tech services. Despite high penetration of mobile-data and smartphones, use for financial transactions is low due to behavioural reasons like lack of trust, misconceptions about taxation, lack of applied knowledge in using digital payment modes and perceived security threats.

The fintech industry has its share of growing pains. However, **the opportunities outweigh the risks**. There's no doubt **fintech will evolve and is here to stay.** Customers will always prefer something that offers a better, affordable experience –from fintech or traditional banks that adapt to provide them.

Cloud Computing

Cloud computing is a technology paradigm that enables individuals and organizations to access and use a wide range of computing resources, including servers, storage, databases, networking, software, and more, over the internet. These resources are hosted and managed by cloud service providers in data centres around the world. Cloud computing offers several

advantages, such as scalability, flexibility, cost-efficiency, and accessibility, making it a popular choice for various applications and services.

The adoption of cloud computing technologies has become a transformative force in the financial services industry, including NBFCs. While the cloud offers numerous benefits, it also presents risks that NBFCs need to address.

Data Sensitivity: NBFCs handle sensitive financial data, making data security and privacy paramount. Storing data in the cloud raises concerns about data breaches, unauthorized access, and data residency issues.

Data Transfer and Portability: Moving data in and out of the cloud, and between different cloud providers, can be technically challenging and time-consuming. Data portability issues may affect NBFCs' operations and ability to switch providers.

Vendor Dependence: NBFCs may become heavily dependent on cloud service providers, making them vulnerable to service disruptions, price changes, or even provider failures.

Regulatory and Compliance Challenges: Regulatory requirements can vary by jurisdiction, and compliance becomes more complex when data is stored in the cloud. NBFCs must ensure that their cloud service providers meet all regulatory standards.

To manage the impact of cloud as an emerging risk, NBFCs can follow:

- Comprehensive Due Diligence: Conduct thorough due diligence when selecting cloud service providers. Assess their security practices, compliance capabilities, and disaster recovery plans. Establish a robust vendor risk management program to monitor and manage the risks associated with cloud service providers.
- Data Security: Understand data residency requirements in various jurisdictions and work with cloud providers that can meet these requirements. Implement strong data encryption measures to protect sensitive information in the cloud.
- Regulatory Adherence: Stay informed about evolving regulations and ensure strict compliance when using cloud services.

Regulatory Changes

The regulatory environment within which NBFCs operate is dynamic, and regulatory changes can pose significant challenges as emerging risks. Regulatory changes encompass alterations in laws, rules, and policies set

forth by regulatory bodies such as the Reserve Bank of India (RBI) and other government agencies. Regulations and legal requirements are continually evolving, and NBFCs must stay abreast of changes to ensure compliance. Regulatory updates can encompass changes in licensing, capital adequacy, risk management, and reporting requirements.

The need to adapt to new regulations often incurs substantial compliance costs related to legal consultations, system upgrades, and employee training. As regulatory requirements become more stringent and detailed, compliance can become more complex, requiring greater attention and resources. Changes in regulations can necessitate substantial operational and procedural adjustments, often requiring considerable financial and human resources. Implementing changes in response to regulatory updates can disrupt day-to-day operations, affecting productivity and efficiency.

Changes in capital adequacy requirements may necessitate additional capital investments, impacting financial stability and profitability.

Evolving regulations may require adjustments to risk management practices, which can be resource-intensive but essential for maintaining a healthy loan portfolio.

To mitigate above risks NBFCs must:

- Establish a robust regulatory monitoring framework to stay informed about impending changes. This allows NBFCs to prepare adequately in advance.
- Implement efficient compliance management systems including tech driven tools and procedures to adapt to evolving regulations in a structured and timely manner.
- Regularly train employees to understand and adhere to updated regulations, ensuring they have the necessary skills and knowledge.
- Engage with regulatory authorities, industry associations, and peers to understand the implications of changes and provide input when possible.

While compliance with updated regulations is essential, proactive management of the risks associated with regulatory changes is equally critical. By adopting a strategic and forward-thinking approach, NBFCs can navigate regulatory changes effectively, ensure compliance, and continue to thrive in the dynamic financial landscape.

Various regulatory guidelines are covered in this Technical Guide.

Environmental, Social, and Governance (ESG)

Environmental, Social, and Governance (ESG) norms are being increasingly viewed as an important factor in how NBFCs are perceived by stakeholders.

Environmental factors refer to the impact of the company's operations on the environment, such as its carbon footprint and efforts to reduce it.

Social factors refer to the company's impact on society, such as its employee practices, diversity, and community involvement.

Governance factors refer to the company's corporate governance policies, such as executive compensation, shareholder rights, and board structure.

The growth of the NBFC sector in India has been driven by many factors, including the increasing demand for credit from businesses and households, the expansion of the financial sector, and the liberalization of the Indian economy. With growth comes the challenges and some NBFCs have raised concerns about the sector's resilience due to deteriorating asset quality.

Given the various risks faced by the sector, there is an increasing need for NBFCs to adopt strong ESG practices. ESG factors can help NBFCs manage risks more effectively and create long-term value for shareholders.

In July 2022, RBI published a Report of the Survey on Climate Risk and Sustainable Finance. Let's look at some pointers from that report.

Climate risk and sustainable finance has caught the attention of regulators, national authorities and supra-national authorities across the world. The Intergovernmental Panel on Climate Change (IPCC) Report of August 2021[9] highlighted the changes being observed in the Earth's climate in every region across the whole climate system. The Report states that emissions of greenhouse gases from human activities are responsible for approximately 1.1°C warming since 1850-1900, and finds that, averaged over the next 20 years, global temperature is expected to reach or exceed 1.5°C warming.

In order to learn from and contribute to the global effort towards enhancing the role of the financial system to manage risks, and in the broader context of environmentally sustainable development, the RBI joined the Central Banks and Supervisors Network for Greening the Financial System (NGFS)[10] as a member in April 2021. Further, the RBI is also represented in the G20 Sustainable Finance Working Group, Financial Stability Board's Working Group on Climate Risk and Work Stream on Climate-related Disclosures, Task Force on Climate-related Financial Risks set up by the Basel

Committee on Banking Supervision (BCBS) and the International Platform on Sustainable Finance.

In May 2021, the RBI set up a sustainable finance group SFG within its Department of Regulations to lead the efforts and regulatory initiatives in the area of climate risk and sustainable finance. The SFG would be instrumental in suggesting strategies and evolving a regulatory framework, including appropriate disclosures, which could be prescribed for banks and other regulated entities (REs) to propagate sustainable practices and mitigate climate-related risks in the Indian context.

a discussion paper (DP) on climate risk and sustainable finance was placed on RBI website on July 27, 2022, for public comments and feedback. Based on analysis of the feedback received in this regard, the RBI has decided to issue several guidelines for Regulated Entities (REs).

These guidelines include:

- Broad framework for acceptance of Green Deposits
- Disclosure framework on Climate-related Financial Risks
- Guidance on Climate Scenario Analysis and Stress Testing

The guidelines will be issued in a phased manner, said Governor Das in his virtual address. They are expected to issue first set of guidelines in current year.

To mitigate the risks posed by ESG factors, NBFCs should adopt a sustainability policy along with systems and procedures to ensure that the company's financing decisions take into account that the borrower's business activities comply with all applicable environmental laws and regulations thereby minimizing environmental impact and promoting sustainable development. By focusing on organizations that work in the field of environmental/ sustainable products or directly funding environment-friendly initiatives, NBFCs can help in the promotion of climate-friendly practices.

NBFCs have an important role to play in financial inclusion in India by targeting last-mile consumers covering people living in rural areas. Lending money to economically backward consumers who do not have access to a good credit score provides a massive growth opportunity in this sector considering a vast potential customer base and simultaneously increasing the living standards and alleviating poverty.

Moreover, by refraining from financing activities that pose social threats e.g. human rights violations, child/ forced labour employment, inadequate labour

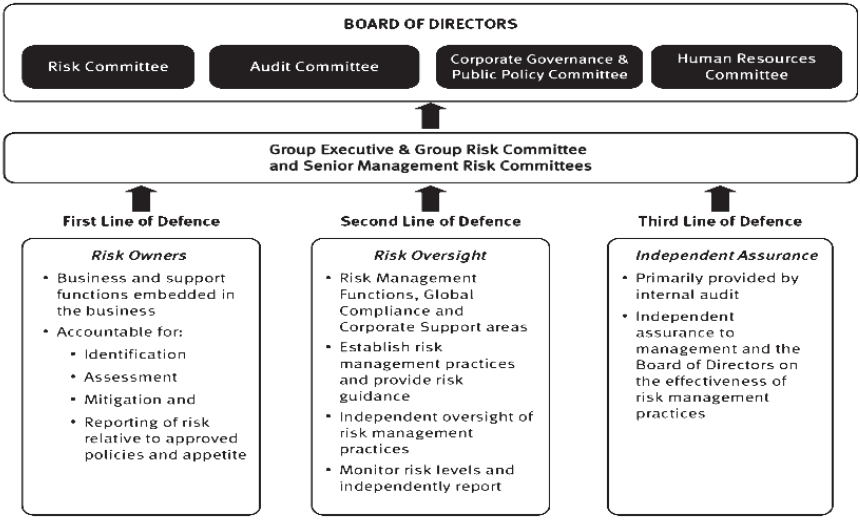
payments, discriminatory employment practices, and unsafe working conditions, NBFCs can avoid their exposure to social and regulatory risks.

NBFCs have a comprehensive and robust governance framework for their organization. To ensure that all the stakeholders including the shareholders, customers, employees, creditors, and regulators are aligned with the organization's objectives. The governance framework will also help the NBFCs to mitigate risks, improve decision making and build a sustainable business. Checking & assessing ESG factors in the course of lending will reduce NBFC's exposure to financial and reputational risks.

Chapter 5
Conducting Risk Based Internal Audit (RBIA)

Understanding Three lines of Defence and Role of Internal Audit in NBFC

5.1 The "Three Lines of Defence" – a risk management framework commonly used in the financial services industry, including Non-Banking Financial Companies (NBFCs). This model helps organizations establish clear lines of responsibility and accountability for managing risks and compliance.



First Line of Defence – Management

5.2 The first line of defence lies with the business and process owners. Business units in an NBFC are primarily focused on generating revenue, but they must do so while adhering to risk management and compliance guidelines. This line of defence plays a crucial role in understanding and managing risks at the operational level.

Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. This consists of identifying and assessing controls and mitigating risks.

Additionally, business and process owners guide the development and implementation of internal policies and procedures and ensure activities are consistent with organisational goals and objectives.

Mid-level managers may design and implement detailed procedures or SOPs (Standard Operating Procedures) that serve as controls and supervise execution by their employees.

Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of the company, its objectives, the environment in which it operates, and the risks it faces.

Second Line of Defence – Risk Management, Compliance and Information Security

5.3 The second line supports management to help ensure risk and controls are effectively managed. Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defence controls.

The second line of defence is responsible for setting policies and procedures, monitoring compliance with regulatory requirements, assessing risk exposure, and providing guidance to the first line of defence.

Typical functions in this second line of defence include Risk Management, Compliance and Information Systems. These functions provide independent oversight and support to the first line of defence.

Risk Management

Risk management function facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.

Its function is to identify, assess, manage, monitor, and report risks. It makes decisions based on a careful risk-return trade-off in line with the defined strategy and with risk appetite.

It should have a strong risk governance (clear organisation structure, well defined roles and responsibilities, documented risk framework), accurate risk and value assessment (identification, quantification and reporting of risks to relevant stakeholders) and prompt risk management actions (timely actions to ensure minimal risk incidents).

Risk Management function ensures that the 1st line of defences implement appropriate risk guidelines in their day-to-day operations.

Compliance

Compliance or regulatory compliance is a term used across industries to describe rules and policies that prohibit or regulate specific products, services, or processes. Simply put, Compliance means abiding by rules, set guidelines or norms which help the society/ industry in general, by creating a harmonize financial, ecological and employment environment.

As 2nd line of defence, compliance function's role in the organisation is to define the Compliance philosophy of the Company by:

- Identifying & assessing a comprehensive compliance framework within which the Company operates including various compliance risks perceived by the Company.
- Developing and maintaining practices that facilitate and consistently monitor compliance within the Company.
- Assisting in assessing and reporting the compliance risk to the relevant authority along with controls/mitigation plans to control/ eliminate such risks.
- Promoting a consistent, effective, rigorous, and comprehensive approach to Compliance throughout the Company.
- Developing and sustaining a culture of compliance where every person within the Company accepts personal responsibility for compliance and acts with the highest standards of ethics and integrity, corporate governance, and accountability.

The Compliance function is distinct from the Risk Management function to independently monitor adherence to statutory/ regulatory requirements, standards of market conduct, managing conflict of interest, treating customers fairly and ensuring the suitability of customer service.

Information Security

Information is a critical asset to a company and Information Security (IS) refers to the protection of these assets to achieve the company's financial and operational goals.

The purpose of IS is to monitor and control the access to sensitive information that resides with the company, ensuring use only by legitimate users so that data and information cannot be read or compromised by unauthorized access.

Through Chief Information Security Officer (CISO), Information Security aims to identify all the risks that the organization faces from an Information Security perspective and strategizes methods to mitigate the identified risks and ensures adherence to business and regulatory requirements.

Third Line of Defence – Internal Audit

5.4 The third line of defence is represented by the internal audit function. This function operates independently from the first and second lines of defence and reports directly to the Audit Committee of the Board.

The third line of defence provides assurance to senior management and the board that the first and second lines efforts are consistent with expectations. The main difference between this third line of defence and the first two lines is its high level of organizational independence and objectivity. Internal Audit may not direct or implement processes, but they can provide advice and recommendations regarding processes. Additionally, Internal Audit may support enterprise risk management but may not implement or perform risk management other than inside of its own function. Internal auditors accomplish their objectives by bringing a systematic approach to evaluating and improving the effectiveness of risk management, control, and governance processes.

While the 3 Line of Defence framework is widely acknowledged and understood by a range of industries as the governance model for risk, its implementation varies in form and maturity. Traditionally, the role of Internal Audit functions is to provide assurance while maintaining objectivity and independence; however, this should be dynamic in nature to keep in line ever changing landscape of business and technology.

Developments in Internal Audit Profession and Standards on Internal Audit (SIAs)

Internal Audit as a profession has seen various changes in past and continues to undergo tremendous changes. Its transformation is becoming more predictive from mere detective, and more analytical from mere verification.

New technologies have created many opportunities to enable a variety of new techniques to be introduced to improve the efficiency and effectiveness of assurance activities. These new approaches have created new opportunities for the Internal Auditor and their future role.

With Artificial intelligence and Machine Learning in foray, Internal Audit now has started thinking on how it can utilize them for its benefit.

The ICAI continues to issue new Standards on Internal Audit (SIAs) to help Chartered Accountants conduct efficient and effective Internal Audits. These SIAs are a set of minimum requirements that apply to all members of the ICAI while performing internal audit of any entity or body corporate.

As per Section 138 of Companies Act, 2013, the Board of a Company may, besides a Chartered Accountant, appoint a cost accountant or any other professional to conduct Internal Audits. The ICAI recommends the adoption of the SIAs by non-members of the ICAI who are performing internal audits so as to ensure a consistent approach and quality in the discharge of their professional duties.

Internal Audit of Critical Areas

5.5 While conducting internal audit of critical areas, following procedure may be followed:

Internal Audit of Sales and Marketing

The Sales and Marketing function in Non-Banking Financial Companies (NBFCs) is the keystone that holds the potential to significantly impact business growth, brand reputation, and customer satisfaction.

The Initial Interface: Bridging NBFCs and Customers

The journey of customer engagement commences with the Sales and Marketing function. It is the frontline that interacts with new customers, introducing them to the myriad financial products and services the NBFC

offers. This initial interaction is more than a mere transaction; it's the cornerstone of a potentially long-lasting relationship built on trust, transparency, and mutual benefit.

Market Research

To remain relevant and competitive, it's imperative for NBFCs to have their finger on the pulse of market trends, customer preferences, and competitive positioning. The Marketing team embarks on a voyage of market research, dissecting various demographics to understand customer needs and preferences. This endeavour extends to analysing competition, pricing strategies, and market positioning, forming a holistic understanding of the market dynamics. The gleaned insights are invaluable, guiding the development of products tailored to meet market demand and ensuring that the NBFC's offerings resonate with the expectations of its target audience.

Engaging Direct Sales Agents (DSAs)

In a bid to manage operational costs without compromising on sales outreach, many NBFCs turn to Direct Sales Agents (DSAs) to operate on their behalf. This strategic engagement allows NBFCs to extend their sales tentacles into various market segments, ensuring a wider reach and a more diverse customer base. DSAs act as the extended arms of the Sales team, representing the NBFC in the market, and playing a crucial role in driving sales numbers.

Sales Process Optimization

An optimized sales process is synonymous with enhanced customer satisfaction. Each stage of the sales process, from lead generation to customer onboarding, is fine-tuned to ensure a smooth, efficient, and enriching experience for the customer. This optimization is not a one-time effort; it's an ongoing endeavour aimed at continuously improving the process in response to feedback and changing market dynamics.

Upholding Compliance: A Non-Negotiable Commitment

Sales and Marketing functions operate within a well-defined compliance framework, delineated by the Compliance team based on various regulatory guidelines. Adherence to this framework is non-negotiable and is ingrained in the ethos of the Sales team. It's not just about following the letter of the law; it's about embracing the spirit of compliance, ensuring that every sales interaction is conducted with the highest degree of integrity and transparency.

Major Risks in Sales and Marketing

The Sales and Marketing function of NBFCs faces a plethora of risks, which, if not managed prudently, can derail the growth trajectory, and tarnish the reputation of the institution.

1. Business Risk – This could be on account of mis-selling amongst other reasons. Mis-selling risk entails the risk of selling unsuitable products or providing misleading information to customers, which is not in their best interest.

2. Reputational Risk: Unethical practices or non-compliance with regulatory guidelines can lead to reputational damage, which can have long-term adverse effects on customer trust and market standing.

3. Regulatory Compliance Risk: Failing to adhere to the myriad of regulatory guidelines set forth by authorities like the RBI can lead to legal repercussions and financial penalties.

4. Data Privacy Risk: The risk of mishandling or misuse of customer data, which can lead to legal liabilities under the IT Act and other data protection laws.

5. Fraudulent Transactions Risk: Instances of fraud in sales transactions or misrepresentation can lead to financial losses and legal issues.

Controls for Mitigating Risks

Implementing a robust control framework is pivotal to mitigating the inherent risks in the Sales and Marketing function.

1. Training and Awareness: Conducting regular training sessions to educate the sales and marketing team on ethical practices, regulatory compliance, and data privacy requirements.

2. Policy Framework: Establishing a well-defined policy framework that outlines the code of conduct, sales protocols, and compliance requirements.

3. Customer Consent and Documentation: Ensuring proper documentation of customer consents, disclosures, and transactions to avoid mis-selling and ensure transparency.

4. Data Protection Measures: Implementing stringent data protection measures to safeguard customer data in accordance with the IT Act and other relevant data protection laws.

5. Regular Monitoring and Review: Conducting regular reviews and monitoring of sales transactions to detect and prevent fraudulent activities and ensure adherence to the established policy framework.

Internal Audit Approach

The Sales and Marketing function is a crucial area where the business strategies intersect with market realities. Given the criticality of this function in Non-Banking Financial Companies (NBFCs), conducting a thorough internal audit is essential to ensure regulatory adherence, financial integrity, and operational efficiency. The audit process should be meticulously designed to align with the Reserve Bank of India (RBI) guidelines, Standards on Internal Audit (SIAs), Companies Act, Prevention of Money Laundering Act (PMLA), Information Technology Act (IT Act), and other applicable laws and regulations.

Risk Assessment and Audit Calendar

- **Risk Assessment:** Ensure that the Risk Assessment has been carried for the function covering all the Inherent Risks & Control Risks of the company.
- **Frequency of Audit**: Based on the severity of the Risk Assessment, the Internal Audit team will determine the frequency of audit and calendarize it.

Audit Planning

- **Scope Definition:** Define the scope of the audit covering all aspects of the Sales and Marketing function, including sales processes, marketing strategies, data handling, and regulatory compliance. Conduct an opening meeting with the stakeholders and perform a process walkthrough.
- **Objective Setting:** Set clear objectives, such as, assessing the effectiveness of controls, verifying regulatory compliance and identifying areas of improvement.
- **Methodology:** Design the audit methodology which could include document reviews, interviews, sampling and testing ensuring it aligns with the RBI guidelines and Standards on Internal Audit.

Control Testing

- **Control Effectiveness:** Evaluate the effectiveness of the controls in place for mitigating risks associated with mis-selling, data privacy, and regulatory non-compliance.

- **Control Efficiency:** Assess the efficiency of the controls in detecting and preventing fraudulent activities, ensuring data integrity, and promoting ethical sales practices.
- **Sales Transactions:** Review the documentation of sales transactions to ensure completeness, accuracy, and compliance with the policy framework.
- **Marketing Campaigns:** Evaluate the documentation of marketing campaigns to ensure alignment with the brand guidelines, regulatory requirements, and ethical practices.

Compliance Verification

- **RBI Guidelines:** Verify adherence to RBI guidelines pertaining to sales and marketing practices, customer interactions, and disclosure requirements.
- **Companies Act Compliance:** Check compliance with the provisions of the Companies Act regarding the conduct of business, customer relations and financial reporting.
- **PMLA Adherence:** Ensure adherence to the PMLA regulations concerning customer identification, record-keeping and reporting of suspicious transactions.
- **IT Act Compliance:** Assess compliance with the IT Act concerning data protection, privacy policies and cybersecurity measures.

Reporting and Recommendations

- **Audit Findings:** Document the findings of the audit, highlighting areas of non-compliance, control weaknesses and operational inefficiencies.
- **Recommendations:** Provide recommendations for improving the control framework, enhancing compliance, and optimizing operational efficiency.

Continuous Monitoring and Improvement

- **Follow-up Audits:** Conduct follow-up audits to verify the implementation of the recommended actions and assess the effectiveness of the corrective measures.
- **Continuous Monitoring:** Establish a continuous monitoring framework to ensure ongoing compliance, control effectiveness and operational efficiency.

- **Training and Awareness:** Propose training programs to enhance awareness and understanding of the regulatory requirements, ethical practices and operational policies among the sales and marketing personnel.

Stakeholder Communication

- **Audit Communication:** Communicate the audit findings, recommendations and corrective action plans to the Audit Committee, the relevant committees, stakeholders ensuring transparency and accountability. Any feedback from the committee or stakeholders should be included in the next audit cycle.

Regulatory Framework for Sales and Marketing Function in NBFCs

The Sales and Marketing function in Non-Banking Financial Companies (NBFCs) is governed by a plethora of laws, regulations and guidelines. Below is a more comprehensive list of relevant acts and guidelines:

Reserve Bank of India (RBI) Guidelines

- **Fair Practices Code (FPC):** Ensuring fair treatment to customers as per RBI guidelines with regard to applications for loans and their processing, loan appraisal and terms/ conditions, disbursement of loans including changes in terms and conditions, general terms, Responsibility of Board of Directors, Grievance Redressal Officer, Ombudsman for NBFCs, Language and mode of communicating Fair Practice Code, Regulation of excessive interest charged by applicable NBFC, Complaints about excessive interest charged by Applicable NBFCs, etc.
- **Know Your Customer (KYC) Guidelines:** Ensuring customer identification and verification processes are in place during customer onboarding.
- **Outsourcing Guidelines:** Adherence to guidelines if sales and marketing functions are outsourced.

Standards on Internal Audit (SIAs)

- **SIA 220 - Conducting Overall Internal Audit Planning:** For planning the internal audit of sales and marketing functions.
- **SIA 320 - Documentation:** For documentation of sales and marketing processes, controls and compliance checks.

Companies Act, 2013

- **Section 134 - Financial Statement, Board's Report, etc.:** For disclosing marketing and sales expenditure and policies.
- **Section 149 - Company to have Board of Directors:** Ensuring ethical sales and marketing practices as per the board's directives.

Prevention of Money Laundering Act (PMLA), 2002

- **Customer Due Diligence (CDD) Procedures:** Adhering to Customer Due Diligence procedures during customer interactions.

Information Technology Act, 2000 (IT Act)

- **Section 43A - Compensation for failure to protect data:** Ensuring data protection in sales and marketing activities.
- **Section 72A - Punishment for Disclosure of information in breach of lawful contract:** Ensuring confidentiality of customer information.

Consumer Protection Act, 2019

- **Various provisions:** Ensuring protection against misrepresentation and misleading information in sales and marketing activities.

Telecom Commercial Communications Customer Preference Regulations, 2018

- **Regulation on Unsolicited Commercial Communication:** Adhering to regulations while conducting marketing campaigns through telecommunication channels.

Advertising Standards Council of India (ASCI) Guidelines

- **Code for Self-Regulation in Advertising:** Ensuring ethical advertising practices.

Foreign Exchange Management Act (FEMA), 1999

- **Various provisions:** If the NBFC is involved in international sales or marketing, compliance with FEMA provisions is crucial.

Goods and Services Tax (GST) Act, 2017

- **Various provisions:** Ensuring compliance with GST provisions in sales and marketing transactions.

Income Tax Act, 1961

- **Various provisions:** Adhering to tax regulations in sales and marketing transactions.

Competition Act, 2002

- **Various provisions:** Ensuring competitive practices in sales and marketing activities.

Insolvency and Bankruptcy Code, 2016

- **Various provisions:** Understanding the implications of insolvency and bankruptcy on sales contracts.

Various Industry-Specific Guidelines

- Adherence to industry-specific guidelines and codes of conduct regarding sales and marketing practices.

Note: Applicability of the above process and regulations would depend upon the products offered, sector of the business entity.

Internal Audit of Know Your Customer (KYC) / Anti Money Laundering (AML) Norms

5.6 In terms of the provisions of Prevention of Money Laundering Act, 2002 (PML Act) and the Prevention of Money Laundering (Maintenance of records) Rules, 2005 (PML Rules), reporting entities (REs) are required to follow Customer Identification Procedures (CIP) while undertaking a transaction at the time of establishing an account-based relationship / client-based relationship and monitor their transactions on-going basis. In this respect, the RBI introduced norms for KYC and AML to be followed by the NBFCs in carrying out business transactions of accepting deposits and lending to customers.

NBFCs are required to frame KYC policy duly approved by the Board of Directors of NBFC or any committee of the Board to which power has been delegated comprising of four key elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures (CIP); and

(d) Monitoring of Transactions.

NBFC need to ensure that the KYC norms/AML standards/CFT measures have been prescribed in the policy and that they ensure that criminals are not

allowed to misuse the banking/financial channels. It would, therefore, be necessary that adequate screening mechanism is put in place by NBFCs as an integral part of their recruitment/hiring process of personnel.

Further Internal audit must refer Standard on Internal Audit (SIA) 150, Compliance with Laws and Regulations as issued by ICAI to understand the responsibilities of internal auditor where compliance activities and framework is a subject matter of an audit, and is being assessed, evaluated and reported on by the Internal Auditor.

Key processes which Internal audit must review during internal audit of KYC & AML compliances:

- Process of Money Laundering and Terrorist Financing Risk Assessment and reporting to the Board
- Customer Acceptance Process (CAP)
- Risk Management covering Customer Risk categorisation, Customer risk rating, periodic reviews
- Customer Identification Procedure (CIP
- Customer Due Diligence (CDD) Procedure
- Employee hiring and employee training process
- Digital and Video-KYC Process
- Procedures for transaction monitoring.
- Monitoring process performed for suspicious transactions & its reporting
- Process implementation to prevent / detect terrorist financing
- Process and controls on ensuring meeting requirements/ obligations under International Agreements
- Communications from International Agencies
- Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967
- Enhanced Due Diligence (EDD) on High-Risk customers and quality of related documentation
- Identification of beneficial owner (BO) as per policy and regulations
- Periodic Updation of KYC

- Enhanced and Simplified Due Diligence Procedure
- Process of reporting to Financial Intelligence Unit - India

Role of Internal Audit

Role of internal audit is to ensure compliance with the policies, procedures and controls relating to the prevention of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction including detection of suspected money laundering transactions. The internal auditor should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. The reports should specifically comment on the robustness of the internal control policies and processes in this regard and make constructive suggestions, where necessary, to strengthen the policy and implementation aspects. Special attention should be paid to business relationships and transactions, especially, those which do not have apparent economic or visible lawful purpose. In such cases, the background and purpose of such transactions must be examined and written findings may be maintained for assisting competent authorities.

Internal Audit Approach

When conducting an internal audit of Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures, it is essential to follow a comprehensive approach. Here are the key steps for consideration:

Planning and Risk Assessment

- Understand the NBFC's business model, size, and customer base.
- Identify inherent risks related to KYC and AML compliance.
- Develop an audit plan based on the identified risks.

Regulatory Compliance Review

- Review and ensure compliance with all applicable laws and regulations governing KYC and AML.
- Check whether the NBFC has updated policies and procedures to reflect any recent regulatory changes.

Policy and Procedure Evaluation

- Examine the NBFC's KYC and AML policies and procedures thoroughly.
- Assess the adequacy of these policies in preventing money laundering and terrorist financing.

- Ensure that KYC procedures are well-documented and align with regulatory requirements.

Customer Due Diligence (CDD)

- Review how the NBFC verifies the identity of customers.
- Evaluate overall adequacy and effectiveness of the Customer Due Diligence program, including policies, procedures, and processes.
- Verify the process for ongoing monitoring of customer transactions.
- Review the customer-risk rating methodology and processes.
- Review a sample of new accounts opening from operating effectiveness.
- Check the adequacy of CDD measures for high-risk customers and periodic high-risk customers review processes.
- Carry out appropriate risk-based transaction testing with respect to the customer profile to verify an adherence to its policies and procedures, record keeping, and reporting requirements.
- Perform risk-based transaction testing with respect to the customer profile to verify an adherence to its policies and procedures, record keeping, and reporting requirements.
- Assess integrity and accuracy of the Management Information System (MIS).
- Perform walkthroughs to understand the knowledge and experience of staff responsible for on boarding customers.
- Evaluate management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations.

Transaction Monitoring

- Evaluate the NBFC's systems for detecting suspicious transactions.
- Ensure that red flag indicators are in place and monitored effectively.
- Check whether reporting mechanisms for suspicious transactions are well-established.
- Assess the integrity and accuracy of the Management Information System (MIS).

Record Keeping

- Ensure that NBFC maintains records of customer details and transactions as required by regulations.

- Review the record-keeping practices to ensure they are accurate and up to date.

Training and Awareness

- Assess the training programs in place for employees regarding KYC and AML.
- Check whether employees are aware of their roles and responsibilities in preventing money laundering.

Testing and Sampling

- Select a sample of customer files and transactions for detailed testing.
- Verify the accuracy of customer information, Customer Due Diligence (CDD) procedures, and transaction monitoring.

Reporting and Communication

- Document audit findings including any deficiencies or non-compliance issues.
- Communicate these findings to senior management and the Board of Directors.

Recommendations and Remediation

- Provide recommendations for addressing identified issues.
- Monitor the implementation of corrective actions.

Follow-Up

- Conduct follow-up audit to ensure that recommended changes have been implemented and are effective.

Documentation

- Maintain comprehensive audit documentation to support the audit process and findings.

During internal audit, it is crucial to maintain independence and objectivity and to keep up-to-date with evolving KYC and AML regulations. Additionally, staying informed about industry best practices is essential to ensure the NBFC's policies and procedures are robust and effective.

Internal Audit of Credit Underwriting and Credit Risk Management Process

5.7 **Credit risk underwriting** can be defined as the assessment of the borrower's personal, financial, or business information to ascertain the

creditworthiness and possibility of failure in the repayment of a loan taken by the borrower. The process involves the verification of KYC documents along with a detailed assessment of the applicant's credit report on well-established benchmarks by the NBFC. It is the amount of risk that an underwriter is willing to accept in exchange for a premium (interest rate). In case the risk is too high, the lender will charge more interest from the Borrower and vice versa. Depending on the type of loan product (Secured or Unsecured) the underwriting process varies. Since NBFCs offer mortgages, loans, credit cards, etc. they need to exercise utmost caution in credit risk analysis and underwriting. All key factors, such as, income, credit history, background and employment checks, Debt to income ratio, security documents, legal and technical valuation reports and so on are considered in this process to assess the risk of lending to the Borrower. Generally, every NBFC has its own Credit policy (also termed as Lending Policy) and is approved by the Board.

Credit Risk Management Process: Credit risk management is a dynamic process and requires continuous re-assessment of the approach in place to prevent adverse impacts in an evolving environment. Key principles of an effective credit risk management process are a forward-looking and a risk-proportionate approach which should be embedded in the end-to-end credit lifecycle.

The C- Conditions for the Underwriting of Risk Assessment

Credit risks, interest rates and premium underwriting are assessed depending on the overall ability of the borrower to adhere to the original contractual terms of loan/ premium repayment. The important 5Cs that any underwriter peruses are:

Capital in business or own contribution of borrowers is important. Higher the cash flows and equity capital lower leverage and better the loan terms.

Capacity to repay instalments or premiums which considers the cash-flow, ability to repay, and terms of repayment.

Conditions of the loan/ obligation depend on economic policies, current market rates, taxes, industry-relevant or economic conditions, the intended use of loan/ premiums and market impact.

Collateral and reputation associated with the loan/policy covered risks associated are important factors in underwriting.

Credit history of parties, how reliable and trustworthy the credit handling has been, foreclosures, bankruptcies, court cases and judgments to be evaluated by lenders while underwriting.

Regulatory challenges and technology developments have been forcing NBFC's to re-examine the cost, efficiency, sustainability, and transparency of their Credit risk management requirements. NBFC's are making use of IT applications and systems to combat these challenges by optimising end-to-end credit underwriting process, for example: .

New modelling techniques – NBFC's are increasingly using Artificial Intelligence/ Machine Learning (AI/ML) models in their credit decisioning processes.

FinTechs – FinTechs are increasingly being used for discrete elements of the end-to-end credit risk journey, from data provision to underwriting platforms.

New MIS and reporting – The new end-to-end credit processes present new inherent risks to the business which need to be identified and incorporated into MIS and reporting. This reporting covers not just credit risk (quantification and early warning) but also operational risk and conduct risk.

Critical areas that the internal audit function should assess during the review of credit underwriting process

Regulatory Compliance: Ensure that the underwriting process adheres to all regulatory requirements and guidelines set by the Reserve Bank of India (RBI) or other relevant authorities.

Credit Risk: This is the most significant risk. Auditors should assess whether the underwriting process accurately evaluates the borrower's ability to repay the loan including income verification, credit history checks and loan-to-value ratios. Internal Audit should confirm that the credit underwriting aligns with the NBFC's credit policy including loan approval authority levels and risk appetite.

Model Risk Management, Credit Scoring Models and Artificial Intelligence: NBFCs are extensively making use of advanced data analytics and modelling techniques to predict credit risk. Internal audit should ensure that data sources are accurate up to date and appropriately used in credit risk models. Internal Audit should review the credit scoring models used to assess the creditworthiness of borrowers. Review the effectiveness and

accuracy of credit scoring models and their calibration to reflect current market conditions. Ensure that these models are robust based on relevant variables and periodically updated. Auditors should also assess and review governance around the use of decisioning models including the length of the historical data used and the modelling techniques (AI/ML, etc.) applied.

Risk Segmentation and Portfolio Diversification: Check whether NBFCs appropriately assess the risk associated with each borrower, considering factors like industry risk, market risk, and economic conditions. Check whether the NBFC segments its customers based on risk profiles. Verify that customers are appropriately categorized to determine the level of risk associated with each segment and assess the diversification of the loan portfolio to reduce concentration risk.

Credit exceptions: Review new/ changed credit underwriting processes and exceptions processes to understand the customer treatment, and the conduct risks associated with this journey.

Loan Review Process: Evaluate the loan review process, including periodic reviews of existing loans to identify signs of deteriorating credit quality. Verify the accuracy and completeness of borrower information and documentation. Ensure that KYC (Know Your Customer) norms are followed.

Credit Monitoring & Early Warning Processes and Fraud Prevention: Assess the effectiveness of ongoing credit monitoring & check if there are monitoring systems in place to track the performance of the loan portfolio and early warning indicators to detect potential credit deterioration. Verify that the underwriting process includes measures to detect and prevent fraud, such as identity theft or income misrepresentation.

Collection and Recovery Procedures: Examine the effectiveness of collection and recovery procedures in case of loan defaults, including the adequacy of provisions and reserves.

Credit Decision Documentation and Record Keeping: Internal audit should review the documentation and record-keeping practices related to credit assessments, approvals, and disbursements to ensure transparency and accuracy Ensure that the rationale for credit decisions is well-documented and that there is a clear audit trail of the decision-making process. Ensure that all necessary loan documents are properly executed and maintained. Verify the completeness of loan files for audits and regulatory purposes.

Credit Committee Oversight: Check the functioning of the credit committee, if applicable, and ensure that it reviews and approves loans within its authority.

Interest Rate Risk: Evaluate how interest rate risk is managed within the loan portfolio, especially in cases of variable rate loans.

Market Risk: Assess how changes in market conditions and economic factors are factored into credit underwriting decisions.

Credit Training and Competence: Confirm that staff involved in credit underwriting have the necessary training and competence to make informed decisions.

Third-Party Vendors: If the NBFC uses third-party vendors for any part of its credit risk management process, audit should evaluate the effectiveness of these relationships and vendor risk management practices.

Credit Loss Provisioning: Assess the adequacy of credit loss provisions based on the assessed credit risk. Ensure that these provisions are made in accordance with accounting standards and regulatory guidelines.

The internal auditor should conduct regular and thorough assessments of these critical areas to help NBFCs effectively manage credit risk and maintain compliance with regulations. Additionally, staying updated with changing regulations and market dynamics is essential for the audit function to provide meaningful insights and recommendations.

Internal Audit of Loan Books Including Expected Credit Loss (ECL)

5.8 The loan book is a critical asset for Non-Banking Financial Companies (NBFCs) embodying the breadth and depth of credit extended to customers. It's a tangible representation of the risk and revenue potential harboured by the institution. The meticulous management of the loan book, intertwined with a robust understanding and application of the ECL model, forms the cornerstone of financial stability and sustainability for NBFCs.

The Loan Book: A Reflection of Credit Activity

The loan book is a comprehensive record of all loan accounts, detailing the amount loaned, repayment schedules, accrued interest, and other pertinent information. It's a dynamic ledger that evolves with every new loan disbursed, every repayment received, and every loan closed. The vitality and quality of the loan book directly impact the NBFC's financial health, revenue generation, and risk profile.

Venturing into Expected Credit Loss (ECL): A Proactive Stance

ECL is a forward-looking model that estimates the likelihood of credit loss over the life of a loan or other financial instruments. It's a proactive approach, shifting away from the "incurred loss" model to recognizing potential losses even before a default occurs. Implementing an ECL model requires a thorough analysis of historical credit data, current economic conditions, and reasonable forecasts of future economic scenarios.

Delineating the Stages of Credit Risk: The ECL Spectrum

Stage 1: At this juncture, the credit risk is deemed to have not increased significantly since the initial recognition. Interest revenue is accrued, and a provision for 12-month ECL is made.

Stage 2: A significant increase in credit risk prompts the shift to Stage 2, where interest revenue continues to accrue, but the provision for lifetime ECL is made.

Stage 3: The credit has deteriorated to the point of credit impairment. Interest revenue is accrued on the net carrying amount (gross carrying amount minus loss allowance).

Constructing a Robust ECL Model: A Blend of Data, Analysis, and Forecasting

Creating an effective ECL model necessitates a blend of historical credit data, meticulous analysis, and prudent forecasting. The model should be adaptable, capable of evolving with changing economic conditions, and regulatory landscapes. It's a blend of quantitative analysis and qualitative insight, all aimed at accurately estimating potential credit losses.

Regulatory Adherence: Aligning with Financial Reporting Standards

The adoption and implementation of the ECL model align with the International Financial Reporting Standard (IFRS) 9 and other financial reporting standards. It's a move towards enhanced transparency, allowing stakeholders to have a clearer understanding of the NBFC's credit risk profile and financial health.

Major Risks

The management of the Loan Book and ECL estimation is fraught with risks that necessitate a robust control and audit framework.

Credit Risk: The likelihood of default on the loans extended by the NBFC, which could lead to financial losses.

Model Risk: Inaccuracies in the ECL estimation model could result in underestimation of credit losses, impacting financial stability.

Regulatory Compliance Risk: Non-compliance with financial reporting standards and regulatory guidelines can lead to legal ramifications and financial penalties.

Data Integrity Risk: Inaccuracies in the data used for ECL estimation can lead to erroneous loss forecasts.

Operational Risk: Inefficiencies in the loan processing, monitoring, and recovery processes can escalate operational costs and credit losses.

Controls for Mitigating Risks

Establishing a robust control framework is instrumental in mitigating the risks associated with Loan Book management and ECL estimation.

Credit Assessment Policies: Implementing stringent credit assessment and approval policies to mitigate credit risk.

ECL Model Validation: Regular validation and back-testing of the ECL model to ensure its accuracy and reliability.

Regulatory Compliance Framework: Establishing a compliance framework to ensure adherence to financial reporting standards, RBI guidelines, and other applicable regulations.

Data Verification Protocols: Implementing protocols for verifying the accuracy and completeness of data used in ECL estimation.

Operational Efficiency Measures: Streamlining loan processing, monitoring, and recovery processes to enhance operational efficiency and reduce credit losses.

Internal Audit Process

The internal audit process is key for ensuring that the controls are effective and the Loan Book and ECL estimation practices are in compliance with the regulatory guidelines.

Risk Assessment and Audit Calendar

Risk Assessment: Ensure that the Risk Assessment has been carried for the particular function covering all the Inherent Risks & Control Risks of the company.

Frequency of Audit: Based on the severity of the Risk Assessment done for the function, the Internal Audit team will determine the frequency of audit & calendarize it.

Audit Planning: Defining the scope, objectives, and methodology of the audit, with reference to RBI guidelines, Companies Act, and other relevant regulations.

Control Testing: Evaluating the effectiveness of the controls implemented for managing the Loan Book and conducting ECL estimation.

Documentation Review: Ensuring that all loan transactions, ECL estimations, and compliance checks are properly documented and retained as per the regulatory requirements.

Compliance Verification: Assessing compliance with the International Financial Reporting Standard (IFRS) 9, Prevention of Money Laundering Act (PMLA), IT Act, and other applicable laws and regulations.

ECL Model Audit: Conducting a thorough audit of the ECL model, including the underlying assumptions, data accuracy, and model validation processes. Ind-AS 109 lays out the guidelines for accounting based on the expected credit loss model. The objective of this standard is to establish reporting principles that will present relevant and useful information to users of financial statements for the assessment of the amount, timings and uncertainty of the entity's future cash flows. This standard will have an impact on the measuring and accounting of credit losses, which means that the risk and finance team of an organization needs to collaborate with the IT department for implementation and complying with Ind-AS 109 standards.

Reporting and Recommendations: Preparing a detailed audit report outlining the findings, recommendations for improvements, and corrective actions required.

Continuous Monitoring and Improvement: Utilizing the audit findings to enhance the control framework, refine the ECL model, and improve the operational efficiency of the loan management processes.

Regulatory Framework for Loan Book Management and Expected Credit Loss (ECL) Estimation in NBFCs

The management of the Loan Book and the estimation of Expected Credit Loss (ECL) in Non-Banking Financial Companies (NBFCs) is a critical function intertwined with a variety of regulatory frameworks. Below is a comprehensive list of relevant acts, standards, and guidelines governing this function:

Reserve Bank of India (RBI) Guidelines

Asset Classification and Provisioning Norms: Guidelines on the classification of assets and provisioning against expected losses.

Prudential Norms on Income Recognition, Asset Classification and Provisioning (IRACP): Guidelines ensuring prudent income recognition and asset classification.

Fair Practices Code (FPC): Guidelines for fair practices while dealing with customers.

Know Your Customer (KYC) and Anti-Money Laundering (AML) Guidelines: Guidelines for customer identification and prevention of money laundering.

Standards on Internal Audit (SIA) as issued by ICAI

SIA 310 - Planning an Internal Audit: Guidance on planning the internal audit of loan book management and ECL estimation.

SIA 320 - Documentation: Guidance on documenting the processes, controls, and compliance checks.

Companies Act, 2013

Section 134 - Financial Statement, Board's report, etc.: Provisions for disclosing ECL and loan book details in financial statements.

Schedule III - General Instructions for preparation of Balance Sheet and Statement of Profit and Loss: Instructions on financial disclosure of loans and provisions.

Prevention of Money Laundering Act (PMLA), 2002

Customer Due Diligence (CDD) Procedures: Requirements for customer identification and verification during loan processing.

Information Technology Act, 2000 (IT Act)

Section 43A - Compensation for failure to protect data: Provisions for protecting customer data during loan processing and management.

International Financial Reporting Standard (IFRS) 9

Financial Instruments: Guidelines for ECL estimation and financial reporting.

Income Tax Act, 1961

Various provisions: Provisions regarding the tax treatment of bad debts, provisions for expected losses, and other relevant tax considerations.

Insolvency and Bankruptcy Code, 2016

Various provisions: Implications of insolvency and bankruptcy on loan recovery and provisioning.

Credit Information Companies (Regulation) Act, 2005

Various provisions: Guidelines for reporting loan information to credit information companies.

Foreign Exchange Management Act (FEMA), 1999

Various provisions: If the NBFC is involved in cross-border lending, compliance with FEMA provisions is crucial.

Securitisation and Reconstruction of Financial Assets and Enforcement of Securities Interest Act (SARFAESI), 2002

Various provisions: Provisions regarding the recovery of loans and enforcement of security interests.

Banking Codes and Standards Board of India (BCSBI) Codes

Code of Bank's Commitment to Customers: Guidelines for fair and transparent dealing with customers.

Various Industry-Specific Guidelines

Adherence to industry-specific guidelines and codes of conduct regarding loan book management and ECL estimation.

Note: Applicability of the above process & regulations would depend upon the products offered, sector of the business entity.

Internal Audit of Assets Liabilities Management

5.9 Assets are resources (tangible and intangible) that your business owns and that can provide you with future economic benefit.

Liabilities are your business' debts or obligations which you need to fulfil in the future. This is the money you need to repay.

An ALM System for the Non-Banking Financial Companies (NBFCs), as part of their overall system for effective risk management in their various portfolios. This guideline would be applicable to all the NBFCs irrespective of whether they are accepting / holding public deposits or not.

NBFCs (engaged in and classified as equipment leasing, hire purchase finance, loan, investment, and residuary non-banking companies) meeting the criteria of asset base of Rs.100 crore (whether accepting / holding public deposits or not) or holding public deposits of Rs. 20 crore or more (irrespective of their asset size) as per their audited balance sheet as of 31 March 2001 would be required to put in place the ALM System.

The ALM process rests on three pillars:

ALM Information System

- Management Information System
- Information availability, accuracy, adequacy, and expediency

ALM Organisation

- Structure and responsibilities
- Level of top management involvement

ALM Process

- Risk identification
- Risk measurement
- Risk management
- Risk policies and tolerance levels

ALM Information System

ALM has to be supported by a management philosophy which clearly specifies the risk policies and tolerance limits. This framework needs to be built on sound methodology with necessary supporting information system as the central element of the entire ALM exercise is the availability of adequate and accurate information with expedience. Thus, information is the key to the ALM process. There are various methods prevalent world-wide for measuring risks. These range from the simple Gap Statement to extremely sophisticated and data intensive Risk Adjusted Profitability Measurement methods. The present guidelines would require comparatively simpler information system for generating liquidity gap and interest rate gap reports.

ALM Organisation

Successful implementation of the risk management process would require strong commitment on the part of the senior management in the FI, to integrate basic operations and strategic decision making with risk

management. The Board should have overall responsibility for management of market risks and should decide the risk management policy of the NBFC and set limits for liquidity, interest rate, exchange rate and equity price risks.

The ALCO (Assets and Liabilities Committee) is a decision-making unit, consisting of the NBFC's senior management including CEO, responsible for integrated balance sheet management from risk-return perspective including the strategic management of interest rate and liquidity risks. While each NBFC will have to decide the role of its ALCO, its powers and responsibilities as also the decisions to be taken by it, its responsibilities would normally include:

- monitoring the market risk levels of the NBFC by ensuring adherence to the various risk-limits set by the Board.
- articulating the current interest rate view and a view on future direction of interest rate movements and base its decisions for future business strategy on this view as also on other parameters considered relevant.
- deciding the business strategy of the NBFC, both - on the assets and liabilities sides, consistent with the NBFC's interest rate view, budget, and pre-determined risk management objectives.
- reviewing the results of and progress in implementation of the decisions made in the previous meetings.

The ALM Support Groups consisting of operating staff should be responsible for analysing, monitoring and reporting the risk profiles to the ALCO. The staff should also prepare forecasts (simulations) reflecting the impact of various possible changes in market conditions on the balance sheet and recommend the action needed to adhere to NBFC 's internal limits.

Composition of ALCO

The size (number of members) of ALCO would depend on the size of each institution, business mix and organisational complexity. To ensure commitment of the Top Management and timely response to market dynamics, the CEO/CMD/DMD or the ED should head the Committee. Though the composition of ALCO could vary across the FIs as per their respective set up and business profile, it would be useful to have the Chiefs of Investment, Credit, Resources Management or Planning, Funds Management/ Treasury (forex and domestic), International Business and Economic Research as the members of the Committee. In addition, the Head

of the Technology Division should also be an invitee for building up of MIS and related computerisation. Some NBFC may even have Sub-committees and Support Groups.

Committee of Directors

The Management Committee of the Board or any other Specific Committee constituted by the Board should oversee the implementation of the ALM system and review its functioning periodically.

ALM Process

- **Risk Identification**

Risk identification (RI) is a set of activities that detect, describe, and catalogue all potential risks to assets and processes that could have negatively impact business outcomes in terms of performance, quality, damage, loss, or reputation.

- **Risk Measurement**

Risk Measurement (also Risk Quantification) is a broad term denoting any activity aiming to quantify (produce numerical measures) risks to an organization. The risks in scope for measurement are normally thought to have been isolated in the Risk Identification process that logical precedes Risk Measurement.

- **Risk Management**

Risk management is the process of identifying, assessing, and controlling threats to an organization's capital, earnings and operations. These risks stem from a variety of sources, including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents, and natural disasters.

- **Risk Policies and Tolerance Levels**

Risk Policy is the set of formal instructions, typically documented and approved by internal governing bodies, that define in sufficient operational detail an organization's perception and attitude towards the range or risks it faces and desires to manage. Risk tolerance refers to the amount of loss an investor is prepared to handle while making an investment decision. Investors are usually classified into three main categories based on how much risk they can tolerate. They include aggressive, moderate, and conservative.

Major Risks involved in ALM Function

Business Risk

Business risk is the exposure a company or organization has to factor(s) that will lower its profits or lead it to fail. Anything that threatens a company's ability to achieve its financial goals is considered a business risk. Arises on account of improper liquidity planning which will impact the business plan of organisations.

Liquidity Risk

By assuring a NBFC ability to meet its liabilities as they become due, liquidity management can reduce the probability of an adverse situation developing.

NBF's management should measure not only the liquidity positions of FIs on an ongoing basis but also examine how liquidity requirements are likely to evolve under different assumptions. Experience shows that assets commonly considered to be liquid, such as Government securities and other money market instruments, could also become illiquid when the market and players are unidirectional.

Legal and Regulatory Risk

It arises if the originator goes bankrupt and there is a possibility that the bankruptcy court may attach the securitised receivables and decide that the pool cash flow should not be specifically earmarked to the investors in the securitisation transactions.

Regulatory Risk is generally defined as the risk of having the 'licence to operate' withdrawn by a regulator, or having conditions applied (retrospectively or prospectively) that adversely impact the economic value of an enterprise.

Reputational Risk

Reputational risk is the damage that can occur to a business when it fails to meet the expectations of its stakeholders and is thus negatively perceived. It can affect any business, regardless of size or industry.

Operational Risk

Operational risk is the potential for losses or damages arising from failures or inadequacies in internal processes, systems, people, or external events. It can affect any business line or function in a bank, such as lending, trading, compliance, IT, or human resources.

People Risk

People Risk' is a topic that can span a whole range of issues for organizations — from individuals making risky or adverse decisions to organizations not quantifying the impact of retirement and knowledge loss. At an even broader level, firms face socio-economic risks like student debt and critical skills gaps.

Controls to be put in place

Governing Control

Establishing a well-defined policy & SOP framework that outlines the processes and compliance requirements.

Preventive Controls

By establishing preventative controls that would provide evidence that an error or irregularity has occurred. to help prevent any irregularities in the process. Liquidity has to be tracked through maturity or cash flow mismatches.

For measuring and managing net funding requirements, the use of a maturity ladder and calculation of cumulative surplus or deficit of funds at selected maturity dates is adopted as standard tool.

Detective Controls

The traditional Gap analysis is a suitable method to measure the Interest Rate Risk in the initial phase of the ALM system. It is the intention of RBI to move over to the modern 10 techniques of Interest Rate Risk measurement like Duration Gap Analysis, Simulation and Value at Risk over time when FIs acquire sufficient expertise and sophistication in acquiring and handling MIS.

Effective Communication

Conducting regular training sessions to educate the respective personnel on regulatory compliance, operational processes involved in ALM Function.

Internal Audit Process

Risk Assessment and Audit Calendar

Make sure Risk assessment of the entire function have been done, based on that Audit frequency of the function will be decided and calendar of the FY to be prepared.

Audit Planning

Scope Definition: Define the scope & Period of the audit covering all aspects of ALM function, including ALM processes, ALM Committee, regulatory compliance.

Objective Setting: Set clear objectives such as assessing the effectiveness of controls, verifying regulatory compliance, and identifying areas of improvement.

Methodology: Design the audit methodology, which could include document reviews, interviews, sampling, and testing, ensuring it aligns with the RBI guidelines and SIAs.

Process Walkthrough of ALM management function.

Review the **Policies and SOP** of ALM Function

Control Testing

Control Effectiveness: Evaluate the effectiveness of the controls in place for mitigating risks associated with ALM function.

Control Efficiency: Assess the efficiency of the controls in detecting and preventing control.

Ensure Compliance with Regulatory norms.

Whether all Assets/ Liabilities have been included in Balance Sheet

Whether all Assets/ Liabilities have been included at correct value

Compliance Verification

RBI Guidelines: Verify adherence to RBI guidelines pertaining to ALM System.

Companies Act Compliance: Schedule of B/S & Disclosures norms as per Companies act.

IND AS: Ensure adherence to Implementation & Disclosures as per IND AS requirements issued by ICAI.

IT Act Compliance: Assess compliance with the IT Act concerning data protection, privacy policies, and cybersecurity measures.

Reporting and Recommendations

Audit Findings: Document the findings of the audit, highlighting areas of non-compliance, control weaknesses, and operational inefficiencies.

Recommendations: Provide recommendations for improving the control framework, enhancing compliance, and optimizing operational efficiency.

Continuous Monitoring and Improvement

Follow-up Audits: Conduct follow-up audits to verify the implementation of the recommended actions and assess the effectiveness of the corrective measures.

Continuous Monitoring: Establish a continuous monitoring framework to ensure ongoing compliance, control effectiveness, and operational efficiency.

Training and Awareness: Propose training programs to enhance awareness and understanding of the regulatory requirements, ethical practices, and operational policies.

Stakeholder Communication

Communicate the audit findings to Audit Committee, recommendations, and corrective action plans to the stakeholders, ensuring transparency and accountability. also, feedback from the audit committee should be considered in determining audit cycle for the next FY.

Internal Audit of Liquidity Management

5.10 Liquidity is blood for any business and more especially in case of NBFCs. NBFCs usually fund their liabilities by leveraging their equity through heavy reliance on market borrowings in the forms of various instruments. Majority of these borrowings are either Commercial Papers, Bank borrowings, External Commercial Borrowings or NCD. NBFCs borrow through these instruments and then continuously refinance these maturing debts through new borrowings from market. As you can see these market borrowing can be accessible only if NBFCs continuously make repayments of maturing debts on due date to provide confidence to market that NBFCs are able to access the markets. *Hence, liquidity planning is very important for any NBFCs due to the continuous need to refinance the debt*. Further, in recent past when one of the biggest NBFC failed in honoring their commitments to markets which resulted in liquidity crisis in Indian market more so for NBFCs as banks and other funds were not willing to lend to them.

In view of these and to make liquidity planning as robust as possible, RBI has introduced a structured way to plan liquidity and introduced various risk management and reporting requirements for each of the NBFCs. It

introduced a Liquidity Risk Management (LRM) framework which focuses on various controls and tolerance limits to strengthen Governance mechanisms and provide enough time to NBFC for planning and knowing in advance the likely shortfall in the liquidity to honors commitments to market participants.

Liquidity Risk Management Policy, Strategies and Practices

Board of the NBFC shall frame a liquidity risk management framework which ensures that it maintains sufficient liquidity including a cushion of unencumbered, high quality liquid assets to withstand a range of stress events.

It shall spell out the entity-level liquidity risk tolerance; funding strategies; prudential limits; system for measuring, assessing and reporting/ reviewing liquidity; framework for stress testing; liquidity planning under alternative scenarios/formal contingent funding plan; nature and frequency of management reporting; periodical review of assumptions used in liquidity projection; etc.

Key elements of the liquidity risk management framework are as under:

Governance of Liquidity Risk Management-involved in the process of identification, measurement and mitigation of liquidity A desirable organisational set up for liquidity risk management should be as under:

Board of Directors, Risk Management Committee, Asset-Liability Management Committee, Asset Liability Management (ALM) Support Group.

Liquidity risk Tolerance-An NBFC shall have a sound process for identifying, measuring, monitoring and controlling liquidity risk.

Liquidity Costs, Benefits and Risks in the Internal Pricing- NBFCs should endeavour to develop a process to quantify liquidity costs and benefits so that the same may be incorporated in the internal product pricing, performance measurement and new product approval process for all material business lines, products, and activities.

Off-balance Sheet Exposures and Contingent Liabilities- The process of identifying, measuring, monitoring, and controlling liquidity risk should include a robust framework for comprehensively projecting cash flows arising from assets, liabilities and off-balance sheet items over an appropriate set of time horizons.

Funding Strategy - Diversified Funding

Collateral Position Management

Stress Testing- Stress testing shall form an integral part of the overall governance and liquidity risk management culture in NBFCs.

Contingency Funding Plan-A n NBFC shall formulate a contingency funding plan (CFP) for responding to severe disruptions which might affect the NBFC's ability to fund some or all of its activities in a timely manner and at a reasonable cost.

Management Information System (MIS)

A NBFC shall have a reliable MIS designed to provide timely and forward-looking information on the liquidity position of the NBFC and the Group to the Board and ALCO, both under normal and stress situations.

Internal Controls

An NBFC shall have appropriate internal controls, systems and procedures to ensure adherence to liquidity risk management policies and procedure. Management should ensure that an independent party regularly reviews and evaluates the various components of the NBFC's liquidity risk management process.

Maturity Profiling

For measuring and managing net funding requirements, the use of a maturity ladder and calculation of cumulative surplus or deficit of funds at selected maturity dates is adopted as a standard tool. The Maturity Profile should be used for measuring the future cash flows of NBFCs in different time buckets.

Liquidity Risk Measurement - Stock Approach

NBFCs shall adopt a "stock" approach to liquidity risk measurement and monitor certain critical ratios in this regard by putting in place internally defined limits as approved by their Board. The ratios and the internal limits shall be based on an NBFC's liquidity risk management capabilities, experience and profile.

Currency Risk

Exchange rate volatility imparts a new dimension to the risk profile of an NBFC's balance sheets having foreign assets.

Managing Interest Rate Risk (IRR)

NBFCs shall manage interest rate risk as per the extant regulatory.

Major Risks

Following major risks involved in Liquidity.

Business Risk

arises on account of improper liquidity planning which will impact the business plan of organisations.

Market Risk

arises on account of change in interest rates.

Liquidity Risk

arises on account of mismanagement of funds, improper business plans and high NPA ratio will impact the liquidity of organizations.

Operational Risk

arises on account of executing transactions, Servicing to investors & borrowers and documentation related to all the transactions.

Regulatory Risk

arises on account of noncompliance to the guidelines issued by regulators, non-reporting to the regulators, non-disclosures.

Reputation Risk

Improper liquidity management will impact the organisation business and credit worthiness which will impact the reputation of organisation.

Controls to be put in place

Implementing a robust control framework is pivotal to mitigating the inherent risks in the liquidity management process.

Governing Control

- Establishing a well-defined policy framework for liquidity risk management that outlines the compliance requirements and guidelines.
- Document the well-defined SOP (Standard operating procedure) consisting of step wise processes and personnel involved in executing transactions and reporting along with defined responsibility.

Preventive Controls

Following preventive measures can be implemented:

- Segregation of duties along with defined approval matrix.
- Maker-checker mechanism for investment & borrowings, authorization & operational activities for accounting.

- Circulating MIS along with impact analyses to the senior management.
- Conducting ALCO meeting as per guidelines issues by the RBI.

Detective Controls

Following are the types of detective controls can be put for auditing of the liquidity management processes:

- Exception reporting in case of any breach in process or incident related to function.
- Reconciliation of loans & investment made.
- Verification of outstanding balance and interest amount on a defined frequency.
- Verification regulatory filling along with all the data sources.
- Monitoring of MIS presented to the ALCO members.

Effective Communication

Conducting regular training sessions to educate the respective personnel on regulatory compliance, operational processes involved in liquidity risk management.

Internal Audit Process

The internal audit process is a critical tool for ensuring that the controls are effective, and respective function operates within the ambit of regulatory compliance and defined policy. Following steps are involved for internal audit process.

Risk Assessment and Audit Calendar

Make sure that risk assessment activity has been carried out for a particular function, based on the severity of risk assessment conducted, Internal Auditor will define the frequency of audit and calendarize it.

Audit Planning

Identify the scope, objectives & methodology of the audit with reference to regulatory guidelines, SIA (Standard on Internal Audit) and entity guidelines.

Conduct an opening meeting with respective heads involved in liquidity management process and raise initial data requirement.

Perform walkthrough of the process and applications involved.

Perform sampling methodology defined in SIA to select the samples for verification.

Testing Controls

Perform testing on the transactions.

Review documentation like agreements, covenants, evidence of registration of executed deals.

Verify the interest working along with all communication for sample months as per sampling methodology.

Verify the data sources and returns filled as per regulatory requirements.

Compliance Check

Make sure all the disclosure as per regulatory guidelines have been disclosed.

Bucket wise reports (Maturity profiling) are prepared as per regulatory guidelines.

GAP analyses and management interest rate risk report is prepared and submitted.

Liquidity coverage ratios are maintained as per guidelines.

Reporting & Follow-up

Conduct closing meeting with relevant stakeholders to discuss and finalise the audit report of function.

Preparing a detailed audit report outlining the findings, recommendations, and corrective actions required.

Ensuring follow-up on the identified issues and monitoring the implementation of corrective actions.

Continuous Improvement

Follow-up Audits: Conduct follow-up audits to verify the implementation of the recommended actions and assess the effectiveness of the corrective measures.

Continuous Monitoring: Establish a continuous monitoring framework to ensure ongoing compliance, control effectiveness, and operational efficiency.

Training and Awareness: Propose training programs to enhance awareness and understanding of the regulatory requirements, ethical practices, and operational policies among the function.

Stakeholder Communication

Communicate the audit findings to the audit committee along with, recommendations, and corrective action plans to the stakeholders, ensuring transparency and accountability.

Any feedback from the audit committee or stakeholders should be included in the next audit cycle.

Provide the feeder to other committees as well as and when particular processes have been not followed or any new controls have been implemented.

Internal Audit of Securitization

5.11 Securitization is a process where a pool of securities is bundled together and are given credit rating by an independent credit agency and then are sold to investors at a fixed coupon rate. Securitization, as the name suggests, involves the transformation of loans, which are a kind of illiquid assets into liquid assets. The underlying assets are generally secured loans such as home loans, automobile loans and unsecured loans like personal loans, etc.

It is a process by way of which an originator (bank) pools together its assets and then sells it to a Special Purpose Vehicle (SPV) – an entity specially created for the process of securitization which further sells it to investors.

Following parties are involved in securitization process.

Originator	Owns the financial assets. Makes loans or receivable from customers.
Obligor/Borrower	Take loan or uses some service of originator.
Investor	Buy the securitization instrument.
Special purpose vehicle (SPV)	Buy assets from originator & packages them into security for further sale.
Facilitators	Enhances the credit worthiness of credit
Credit Rating Agencies	Provide rating to the product.
Insurance Companies	Act as underwriters and provide cover for the redemption risk to the investor.
Trustee	Oversee the performance of other parties involved.

Types of Securitizations

Pass-Through Certificates (PTC's)

Pass-Through Certificates are similar to bonds, the difference being that they are issued against underlying securities. The payment to investors constitutes interest payments and principal payments received by the obligator on a pro-rata basis after deducting the servicing fee. However, in a Pay-Through Certificate, the principal and the interest amount are not transferred to the investor. Instead, the investors are issued new securities by SPV in return to this.

Direct Assignment

Direct Assignment involves buying a loan book at a fixed interest rate. Suppose a bank is interested in increasing his exposure to agricultural loan, to fulfil this, he will directly buy the pool of agrarian loan from an NBFC. Here, the terms are negotiable and can be customized in Favour of both parties.

Major Risks

Securitization is an easy way out for NBFC's, to transfer their pool of illiquid assets to banks in order to convert them into tradeable securities. However, to ensure that NBFC's do bear some risk even after the Securitization Process, the concept of Minimum Retention Ratio (MRR) was brought forward. This means if a part of the loan pool goes into default, the first blow will be borne by the originator (NBFC's).

The RBI guideline dated November 29, 2018, states that loans which have an original maturity of 5years, or above which receive six monthly instalments or two quarterly instalments, the MRR requirements would be 20% of the book value of the loans being securitised/20% of the cash flows from the assets assigned.

Following major risks involved in securitization process.

Credit Risk

arises on non-payment by underlying borrowers in the pool of loans because of the inability or unwillingness to pay. Analysis of the nature of the underlying asset class, robustness of the origination processes, past performance of the originator's overall portfolio and pool characteristics will provide pertinent insights into the credit risk associated with the underlying borrowers.

Legal Risk

arises if the originator goes bankrupt and there is a possibility that the bankruptcy court may attach the securitised receivables and decide that the pool cash flow should not be specifically earmarked to the investors in the securitisation transactions.

Market Risk

arises on account of factors external to securitisation transactions such as prepayment of loans, movement in interest rates and macroeconomic factors.

Operational Risk

arises on account of executing transactions, pay-out, Servicing to investors and documentation related to deals.

Controls to be put in place

Implementing a robust control framework is pivotal to mitigating the inherent risks in the securitization process.

Governing Control

Establishing a well-defined policy framework for securitization that outlines the compliance requirements and guidelines.

Document the well-defined SOP (Standard operating procedure) consisting of step wise processes and personnel involved in executing transactions along with defined responsibility.

Preventive Controls

Following preventive measures can be implemented.

- Following the steps defined in SOP.
- Segregation of duties along with defined approval matrix.
- Maker-checker mechanism for selection of pool, authorization & payout activities.

Detective Controls

Following are the types of detective controls can be put.

- Auditing of deals on sample basis
- Exception reporting in case of any breach in process or incident related to securitization.

- Reconciliation of loan book vis-à-vis MIS.
- Payout working verification on a defined frequency, confirmation from the other party.

Effective Communication

Conducting regular training sessions to educate the respective personnel on regulatory compliance, operational processes involved in securitizations.

Internal Audit Process

The internal audit process is a critical tool for ensuring that the controls are effective, and respective function operates within the ambit of regulatory compliance and defined policy. Following steps are involved for internal audit process.

Risk Assessment and Audit Calendar

Make sure that risk assessment activity has been carried out for a particular function, based on the severity of risk assessment conducted, Internal Auditor will define the frequency of audit and calendarize it.

Audit Planning

Identify the scope, objectives & methodology of the audit with reference to regulatory guidelines, SIA (Standard on Internal Audit) and entity guidelines.

Conduct an opening meeting with respective heads involved in securitization of process and raise initial data requirement.

Perform walkthrough of the process and applications involved.

Perform sampling methodology defined in SIA to select the samples for verification.

Testing Controls

Perform testing on the samples selected for transactions which had been securitized.

Review documentation like agreements, evidence of registration of executed deals.

verify the payout working along with all communication for sample months as per sampling methodology.

Compliance Check

Make sure all the disclosure as per regulatory guidelines have been disclosed.

Minimum retention ratio has been kept for all the deals executed as per guidelines issued by RBI.

Reporting & Follow-up

Conduct closing meeting with relevant stakeholders to discuss and finalise the audit report of function.

Preparing a detailed audit report outlining the findings, recommendations, and corrective actions required.

Ensuring follow-up on the identified issues and monitoring the implementation of corrective actions.

Continuous Improvement

- **Follow-up Audits:** Conduct follow-up audits to verify the implementation of the recommended actions and assess the effectiveness of the corrective measures.
- **Continuous Monitoring:** Establish a continuous monitoring framework to ensure ongoing compliance, control effectiveness, and operational efficiency.

Training and Awareness: Propose training programs to enhance awareness and understanding of the regulatory requirements, ethical practices, and operational policies among the function.

Stakeholder Communication

Communicate the audit findings to the audit committee along with, recommendations, and corrective action plans to the stakeholders, ensuring transparency and accountability.

Any feedback from the audit committee or stakeholders should be included in the next audit cycle.

Provide the feeder to other committees as well as and when processes have been not followed or any new controls have been implemented.

Following material can be used as reference for various guidelines issued by the regulators on securitization.

Internal Audit of Outsourcing Management including IT Outsourcing

Outsourcing of Financial Services

5.12 In order to get access to specialist expertise and to reduce operational costs, Non-Banking Financial Companies (NBFCs) extensively outsource some of their operations. These outsourced activities were hitherto not regulated and hence, exposed the NBFCs as well as their customers to considerable risks, such as strategic risk, reputation risk, compliance risk, operational risk, legal risk etc. Hence, a need was felt to put in place appropriate safeguards for addressing these risks. RBI issued Directions on Managing risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Companies on November 09, 2017 with a view to lay down a framework for outsourcing for NBFCs.

The directions are applicable to material outsourcing arrangements and relate to managing risks in the outsourcing of financial services. The directions are not applicable to technology related issues and activities not related to financial services, such as using couriers, housekeeping, security of premises, movement and archiving of records, etc.

If the NBFC uses service organizations to provide core services or activities, such as, cash and securities settlement or back-office activities the responsibility for compliance with rules and regulations and sound internal controls remains with those charged with governance and the management of the outsourcing NBFC. The internal auditor should consider legal and regulatory restrictions and obtains an understanding of how the management and those charged with governance monitor that the system of internal control (including internal audit) operates effectively. SA 402, "Audit Considerations Relating to an Entity Using a Service Organization" gives further guidance on this subject. Additionally, ICAI has issued Standard on Internal Audit (SIA) 530, Third Party Service Provider. SIA 530 deals with the responsibility of the Internal Auditor and management with regard to risks arising from situations where some parts of the entity's business operations, processes and information reside with Third-Party Service Providers (TPSPs).

Regulatory mandate: As per RBI directions on Managing risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Companies in November 09, 2017

- A robust system of internal audit of all outsourced activities shall also be put in place and monitored by the Audit Committee of the NBFC
- Regular audits shall assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the NBFC's compliance with its risk management framework and the requirements of these directions.

When conducting an internal audit of managing risks and the code of conduct in outsourcing of financial services by a Non-Banking Financial Company (NBFC), there are several critical areas that should be carefully examined. Here are some key points to consider:

1. Risk Management Framework: Assess the NBFC's risk management framework for outsourcing. Ensure it complies with regulatory guidelines and industry best practices. This includes risk assessment, risk mitigation, and risk monitoring processes.

2. Due Diligence of Service Providers: Examine the NBFC's due diligence process for selecting outsourcing service providers. Verify that background checks, financial stability assessments, and legal compliance checks are conducted.

3. Contractual Agreements: Review outsourcing contracts and agreements thoroughly. Ensure that they define roles, responsibilities, service levels, data protection measures, and exit strategies clearly. Check for compliance with regulatory requirements.

4. Data Security and Privacy: Audit the measures in place to protect sensitive customer data and ensure compliance with data protection regulations. Assess the encryption, access controls, and data retention policies of the outsourcing partner.

5. Code of Conduct: Evaluate the NBFC's code of conduct and ethical guidelines. Verify that these guidelines are communicated to the outsourcing partner and are adhered to throughout the relationship.

6. Compliance with Regulations: Ensure that the outsourcing activities comply with all relevant regulatory requirements, such as those outlined by the Reserve Bank of India (RBI) or other applicable authorities.

7. Monitoring and Reporting: Assess the NBFC's monitoring mechanisms for outsourced activities. Verify that there are regular reports and key performance indicators (KPIs) in place to track the performance and risk exposure of the outsourcing partner.

8. Contingency Planning: Check for the existence of contingency plans and disaster recovery measures in case the outsourcing partner faces disruptions or fails to meet service level agreements.

9. Audit Trails and Documentation: Review documentation related to outsourced activities, including audit trails and records of transactions. Ensure that documentation is maintained according to regulatory standards.

10. Training and Awareness: Assess whether the NBFC provides adequate training and awareness programs to employees regarding the code of conduct and risk management associated with outsourcing.

11. Exit Strategy: Verify that there is a well-defined exit strategy in case the outsourcing arrangement needs to be terminated. Ensure that data and operations can be smoothly transitioned back in-house or to another service provider.

12. Third-Party Audit: Consider engaging a third-party audit firm or specialist to conduct an independent audit of the outsourcing arrangements for an objective assessment.

13. Continuous Improvement: Encourage the NBFC to have mechanisms in place for continuous improvement in managing risks and code of conduct in outsourcing. Recommendations from audits should be used to enhance practices.

IT Outsourcing

The Reserve Bank of India (RBI) has issued a Master Direction on outsourcing of information technology services by REs on 10 April 2023. The Directions apply to 'material outsourcing of information (IT) services', defined as services which:

(i) if disrupted/ compromised have the potential to significantly impact the business operations of RE; and

(ii) may have material impact on RE' customers if there is any unauthorised access, loss or theft of customer information.

Regulatory mandate: As per RBI "RE's shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by RE's internal auditors or external auditors appointed to act on RE's behalf. The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by

the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact to the RE from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management and in case of any adverse development, the same shall be put up to the Board for information.

Internal Audit Process

When conducting an Internal audit of IT outsourcing it is suggested to review the applicable regulatory guidelines for adherences. There are several critical areas/ processes that should be carefully examined Here are some of the key processes which should be assessed by internal audit.

i. Grievance redressal framework and Process: The responsibility of customer grievance redressal must rest with the NBFC.

ii. Governance Framework: Board-approved comprehensive IT outsourcing policy, governing the roles and responsibilities of the board, committees of the board, senior management, IT function, business function, oversight and assurance functions in respect of outsourcing of IT services must be put in place.

iii. Due diligence on Service Providers: NBFC must conduct due diligence on third party service provider based on a risk-based approach, taking into consideration various qualitative, quantitative, legal, reputational and operational factors, along with associated risks.

iv. Monitor/ Control: NBFC must conduct periodic audits to assess key factors such as performance of service providers, risk management activities adopted, etc.

v. Risk Management Framework: NBFC must put in place a robust risk management framework, including the identification, measurement, mitigation/ management and reporting of risks.

vi. Confidentiality and Security: NBFC must also be responsible for ensuring that customer data with third party service providers are secure and confidential, with access on a need-to-know basis.

vii. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP): Third party service providers must have an established framework for BCP and DRP.

viii. Outsourcing to Business Group/ Conglomerate: On the condition that a board-approved policy is in place, NBFC can outsource IT activities to its business group/ conglomerate.

ix. Security Operations Centre ("SOC"): Outsourcing of operations to an SOC may carry certain risks, particularly since the data is not only stored and processed at an external location, but also managed by a third party.

x. Reporting of Cyber Incidents: NBFC should ensure that cyber incidents are reported to them by their service providers without undue delay, so that the same can be reported by the REs to the RBI. NBFC's are also required to monitor the Service Provider's control processes and security practices to disclose security breaches, and immediately notify the RBI in case of any breach of security and leakage of confidential customer information.

xi. Constituents of the Outsourcing Agreement: NBFC should ensure that the rights and obligations of the NBFC and their Service Providers are clearly set out in a legally binding written agreement, duly vetted by the NBFC legal counsel.

xii. Internal Audit of Customer Service

The customer service plays a crucial role in any Non-Banking Financial Company (NBFC) in India for several reasons:

- **Customer Satisfaction:** Ensuring a high level of customer satisfaction is vital for retaining existing customers and attracting new ones. Happy customers are more likely to continue doing business with the NBFC and recommend it to others.
- **Compliance with Regulatory Requirements:** NBFCs in India are subject to strict regulatory requirements set by the Reserve Bank of India (RBI) and other authorities. These regulations often include guidelines for customer service, such as grievance redressal mechanisms and fair lending practices. Compliance is essential to avoid penalties and maintain the company's reputation.
- **Risk Management:** The customer service helps identify and mitigate operational and reputational risks. Promptly addressing customer complaints and concerns can prevent these issues from escalating and damaging the company's standing.
- **Business Growth:** A positive customer service experience can lead to increased customer loyalty and word-of-mouth referrals, contributing to business growth and profitability.

Over a period of years, the customer service function has undergone a significant transformation driven by technological advancements. This technical guide explores the evolution of customer service within NBFCs, highlighting the key trends and strategies that have reshaped the industry.

1. **Digitalization and Automation:** The digital revolution has been a game-changer for NBFCs' customer service. Automated chatbots and AI-driven virtual assistants are now commonly used to handle routine customer queries, improving efficiency and response times.

2. **Data-Driven Insights:** Customer data analytics has become indispensable for NBFCs. By harnessing the power of big data, NBFCs can personalize services, predict customer needs, and proactively address issues.

3. **Omnichannel Communication:** NBFCs have adopted an omnichannel approach to cater to diverse customer preferences. This includes seamless integration of phone, email, chat, and social media platforms, ensuring a consistent and convenient customer experience.

4. **Self-Service Portals:** Many NBFCs now offer self-service portals and mobile apps, allowing customers to access their accounts, make transactions, and resolve common issues independently, reducing the need for direct customer support.

5. **Enhanced Security Measures:** With the rise in cyber threats, NBFCs have invested heavily in cybersecurity to protect customer data. Multi-factor authentication, encryption, and continuous monitoring are standard practices.

6. **Regulatory Compliance:** Customer service in NBFCs now closely aligns with stringent regulatory requirements. This includes robust KYC (Know Your Customer) processes, data privacy compliance, and transparent communication with customers regarding policies and terms.

7. **Personalization at Scale:** Leveraging AI and machine learning algorithms, NBFCs can personalize their offerings and communications, tailoring products and services to individual customer needs and preferences.

8. **24/7 Availability:** To accommodate global customers and provide round-the-clock support, many NBFCs offer 24/7 customer service through various channels, ensuring assistance is available when needed.

9. **Feedback Loops:** NBFCs actively seek customer feedback and use it to drive continuous improvement in their services. Customer feedback

surveys, online reviews, and social media monitoring play a crucial role in shaping the customer service function.

10. Training and Upskilling: In light of these technological advancements, NBFCs invest in training and upskilling their customer service teams. Employees must stay updated on the latest technology trends and customer service best practices.

Internal Audit Process

As the customer service function in NBFCs undergoes significant transformation, internal audit teams must adapt to effectively audit this area. Here are key areas that should be audited to ensure compliance, efficiency, and effectiveness in the evolving customer service landscape:

1. Technology Infrastructure and Security: Audit teams should assess the NBFC's technology infrastructure, including servers, databases, and communication systems. Ensure that cybersecurity measures are in place to protect customer data and sensitive information from cyber threats.

2. Data Handling and Privacy Compliance: Auditors should verify that the NBFC complies with data privacy regulations and standards. This includes auditing the collection, storage, processing, and sharing of customer data, as well as the organization's adherence to GDPR, HIPAA, or other applicable data protection laws.

3. Automation and Chatbots: Audit teams must evaluate the deployment and performance of automated chatbots and virtual assistants. Ensure that these technologies are providing accurate and helpful responses to customers and that they are well-monitored for potential issues.

4. Omnichannel Integration: Verify the seamless integration of customer service across various channels, such as phone, email, chat, and social media. Confirm that customers receive consistent service and information regardless of the channel they choose.

5. Compliance with Regulatory Requirements: Assess whether the NBFC complies with regulatory requirements governing customer service, including KYC, AML (Anti-Money Laundering), and customer disclosure mandates. Ensure that customer communication and interactions align with these regulations.

6. Self-Service Portals and Apps: Audit the functionality and security of self-service portals and mobile apps. Confirm that customers can access

their accounts securely and that these platforms provide accurate information and transaction capabilities.

7. Customer Feedback and Complaint Handling: Evaluate how customer feedback and complaints are collected, analysed, and addressed. Ensure that there is a robust system in place to address customer concerns promptly and effectively.

8. Training and Skill Development: Audit the training and skill development programs for customer service teams. Ensure that employees are equipped with the necessary skills to handle evolving technologies and provide exceptional service.

9. Continuous Improvement and Monitoring: Assess the NBFC's approach to continuous improvement in customer service. Ensure that key performance indicators (KPIs) are monitored, and feedback from audits and customer interactions is used to make necessary adjustments.

10. Disaster Recovery and Business Continuity: Audit the NBFC's disaster recovery and business continuity plans for customer service operations. Ensure that there are contingency measures in place to address technical failures or disruptions.

11. Vendor and Third-Party Management: If the NBFC relies on third-party vendors for customer service technology or support, assess vendor relationships and contracts to ensure compliance and reliability.

12. Ethical Considerations: Audit teams should also consider ethical aspects of customer service, ensuring that practices are fair, transparent, and aligned with the company's values and code of conduct.

Incorporating these key areas into the internal audit process will help NBFCs ensure that their customer service function remains compliant, efficient, and capable of meeting the evolving needs of customers in the digital age. Auditors must adapt their methodologies to effectively evaluate these areas and provide valuable insights for the organization's success.

Internal Audit of Finance & Accounts

5.13 Finance and accounting are critical areas for Non-Banking Financial Companies (NBFCs) in India. Ensuring the accuracy, transparency, and compliance of financial operations is essential for the stability and reputation of these institutions. When conducting an internal audit of the finance function and application systems in an NBFC in India, several key considerations should be kept in mind:

1. **Regulatory Compliance**: NBFCs in India are subject to regulations issued by the Reserve Bank of India (RBI). Ensure that all financial operations comply with the RBI guidelines, including those related to capital adequacy, income recognition, asset classification, and provisioning norms.

2. **Financial Statements**: Review financial statements for accuracy and compliance with Indian Accounting Standards (Ind AS). Check for any inconsistencies or errors in financial reporting, including balance sheets, income statements, and cash flow statements.

3. **Asset Quality**: Assess the quality of assets by examining the loan portfolio. Ensure that proper due diligence is conducted before lending, and loan classification and provisioning norms are followed as per RBI guidelines.

4. **Income Recognition**: Verify that income is recognized as per the RBI guidelines and accounting standards. Ensure that interest income, fees, and other charges are recognized appropriately.

5. **Internal Controls**: Evaluate the internal controls in place to safeguard financial assets and prevent fraud. Ensure segregation of duties, authorization limits, and access controls are effectively implemented.

6. **Reconciliation**: Perform regular reconciliations of financial data between various systems and records to identify discrepancies.

7. **Documentation**: Ensure that all financial transactions are properly documented, and records are maintained as required by regulatory authorities.

8. **Risk Management**: Assess the NBFC's risk management practices, including credit risk, liquidity risk, and market risk. Ensure that risk assessments are regularly conducted, and risk mitigation measures are in place.

9. **Reporting**: Review the accuracy and timeliness of regulatory reporting to the RBI. Ensure that all required reports are submitted within the stipulated timelines.

Internal Audit Process

During the internal audit, it's important to document findings, assess the adequacy of existing policies and procedures, and recommend improvements where necessary. Continuous monitoring and periodic audits are essential to ensure that the finance function of the NBFC remains compliant with regulatory requirements and maintains the highest standards of financial

integrity.

System controls in finance and accounting systems, along with audit trail requirements and system integration, are critical aspects of ensuring the accuracy, security, and compliance of financial data. Here's an overview of these components:

1. System Controls in Finance and Accounting Systems:

- **IT Systems**: Examine the reliability and security of IT systems used in financial operations. Ensure that these systems are up-to-date, well-maintained, and have appropriate disaster recovery plans.
- **Access Controls:** Implement role-based access controls to ensure that only authorized personnel can access sensitive financial data and perform specific actions. This helps prevent unauthorized changes or fraud.
- **Data Validation and Verification:** Implement data validation checks to ensure the accuracy and integrity of data entered into the system. This includes checks for data completeness, accuracy, and consistency.
- **Data Security**: Review data security measures for finance applications. Sensitive financial data must be protected from unauthorized access or breaches. Assess the adequacy of encryption, access controls, and data backup processes.
- **Segregation of Duties (SoD):** Define and enforce clear roles and responsibilities within the finance and accounting system. This prevents any single individual from having too much control over critical financial processes, reducing the risk of fraud or errors.
- **Change Management:** Establish controls over system changes, updates, or modifications to ensure that they are thoroughly tested and approved before implementation. Changes should be documented and tracked.
- **Encryption and Data Security:** Protect sensitive financial data through encryption both in transit and at rest. Implement cybersecurity measures to guard against data breaches and unauthorized access.
- **Backup and Recovery:** Regularly back up financial data and create disaster recovery plans to ensure business continuity in case of system failures or data loss.

2. Audit Trail Requirements:

- An audit trail is a chronological record of all activities and transactions within the finance and accounting system. It serves as a detailed history that can be reviewed for various purposes, including compliance, investigation, and accountability.
- Audit trails should capture details such as user IDs, timestamps, actions taken (e.g., data entry, modification, deletion), and the specific data involved.
- The audit trail should be tamper-proof, meaning that once a record is created, it cannot be altered by users without proper authorization.
- Retention policies should be established to determine how long audit trail records are kept, ensuring compliance with regulatory requirements.

3. System Integration:

- Finance and accounting systems often need to integrate with other enterprise systems, such as ERP (Enterprise Resource Planning) systems, CRM (Customer Relationship Management) systems, and banking platforms.
- Integration allows for the seamless flow of data between systems, reducing manual data entry, improving accuracy, and enhancing efficiency.
- Data mapping and data transformation processes should be well-documented to ensure that data is transferred accurately between systems.
- Integration should also consider security and access controls to protect data as it moves between systems.

It's important to note that compliance requirements, security standards, and best practices may evolve over time, so finance and accounting systems should be regularly reviewed and updated to meet current standards. Additionally, internal audits play a crucial role in evaluating the effectiveness of system controls and audit trail requirements.

Internal Audit of Governance and Compliance

5.14 The compliance function in Non-Banking Financial Companies (NBFCs) plays a crucial role in ensuring that the company adheres to regulatory and legal requirements. Here are some of its key responsibilities:

Regulatory Compliance: Ensuring that the NBFC complies with all applicable laws, rules, and regulations set by regulatory authorities such as the Reserve Bank of India (RBI) or other relevant bodies.

Policies and Procedures: Developing, implementing, and maintaining policies, procedures, and controls to ensure compliance with regulatory requirements and internal standards.

Risk Assessment: Identifying and assessing compliance-related risks and developing strategies to mitigate them.

Reporting: Preparing and submitting regular reports to regulatory authorities as required by law.

Training and Awareness: Providing training and awareness programs to staff members to ensure they understand and comply with regulatory requirements.

Monitoring and Testing: Continuously monitoring and testing the NBFC's operations to ensure ongoing compliance and identifying any potential issues or violations.

Remediation: Taking corrective actions when compliance violations are identified, including reporting to senior management and regulatory authorities when necessary.

Internal Audit Process

When conducting an internal audit of the compliance function within an NBFC, critical areas to audit include:

Risk Assessment: Assess the processes in place for identifying, assessing, and mitigating compliance risks, and ensure that risk assessments are regularly updated.

Compliance Policies and Procedures: Review the adequacy and effectiveness of the company's compliance policies and procedures, ensuring they are up to date and followed consistently.

Regulatory Adherence: Verify that the processes and controls instituted by the NBFC in complying with all applicable laws, regulations, and guidelines, including those related to capital adequacy, lending practices, and customer protection.

Record Keeping: Ensure that the NBFC maintains accurate and complete records of all compliance-related activities, including documentation of regulatory filings.

Reporting: Review the process and controls around submission of reports to regulatory authorities on time and with accurate information.

Training and Awareness: Evaluate the effectiveness of training programs and the level of compliance awareness among employees.

Monitoring and Testing: Review the processes for ongoing monitoring and testing of compliance controls and the documentation of findings and remediation actions.

Compliance Culture: Assess the overall compliance culture within the organization, including the tone set by senior management and the commitment to ethical behaviour and regulatory compliance.

Escalation and Reporting: Check that there is a clear process for escalating compliance issues and reporting them to senior management and regulatory authorities when necessary.

An effective internal audit of the compliance function helps ensure that an NBFC operates within the bounds of the law and regulatory requirements, reducing the risk of legal and financial penalties and maintaining the trust of stakeholders.

Internal Audit of Risk including Fraud and Irregularities

Standard on Internal Audit 130, Enterprise Risk Management

Standard on Internal Audit (SIA) 130 Risk Management* issued by the ICAI, seeks to clarify the concept and also the responsibility of the Internal Auditor, Management and other Stakeholders with respect to risk management, keeping in mind the legal, regulatory and professional obligations.

SIA 130 Provide the guidance as given below:

Para	Standards
4.0	**Responsibility of the Board and Management**
4.1	The responsibility of the Board of Directors in the areas of Risk Management is, generally, established by the prevailing laws of the nation. The responsibility of the management is established

	by both the prevailing laws and the oversight of the Board of Directors.
4.5	Overall responsibility for developing, implementing and monitoring of risk management rests with the Board of Directors, risk management department and Management and should be appropriately covered in the internal audit scope.
5.	**Responsibility of the Internal Auditor**
5.1	Unless specially excluded from the audit approach, the Internal Auditor shall plan and conduct risk based internal audits. This requires the application of risk management concepts to ensure that the audits are prioritized in areas of importance, appropriate resources are allocated effectively where needed most, audit procedures are designed to give due attention to important matters and issues identified and reported are significant in nature (refer Para 6.1 of SIA 130, provided below).
5.2	The nature and extent of audit procedures to be conducted in the area of risk management is dependent on the maturity of the risk management processes and the framework in place. Where management has implemented a risk management framework, the Internal Auditor shall plan and perform audit procedures to evaluate the design, implementation and operating effectiveness of the organisation's risk management framework to provide independent assurance to management and those charged with governance (refer Para6.2 and Para 6.3 of SIA 130, provided below).
5.3	Where formal risk management framework exists, the Internal Auditor shall design and conduct audit procedures with a view to highlight any exposures arising from weak or absent risk management activities, make recommendations to implement and strengthen related processes and thereby improve risk management (refer Para 6.4 of SIA 130, provided below).
5.4	Where the independent assurance requires the issuance of an audit opinion over the design, implementation and operating effectiveness of risk management, this shall be undertaken in line with the requirements of SIA 110, "Nature of Assurance", especially with regard to the need to have a formal Risk Management Framework in place, which shall form the basis of such an assurance (refer Para 6.5 provided below).

5.5	The Internal Auditor shall not assume any responsibility to manage the risks or to execute risk management decisions. It is not responsibility of the Internal Auditor to mitigate or resolve the risks.
6.0	**Explanatory Comments:**
6.1	**Risk Based Internal Audit (refer Para 5.1 provided above):** Para 3.6 of "Basic Principles of Internal Audit" on Risk Based Audits, requires the Internal Auditor to conduct the audits based on a risk assessment exercise. SIA 220, "Conducting Overall Internal Audit Planning" and SIA 310, "Planning the Internal Audit Assignment" mandate the Internal Auditor to conduct risk-based audit planning to ensure that due attention is given to matters of importance, complexity and sensitivity. Similarly, SIA370, "Reporting Results" expects the auditor to consider the risk of the observations in deciding the matters to be reported.
6.2	**Audit Objectives on Risk Management Framework (refer Para 5.2 provided above):** The Internal Auditor shall perform audit procedures over the risk management framework with an overall objective to review the organisation's ability to: Identify all risks; Assess the objectively; Respond to them through controls or other mitigations; Ensure unmitigated risks are within the tolerance level; and Monitor and report their status in a timely manner to enable achievement of organisational objectives. The Internal Auditor will review the risk management system and processes in place to evaluate whether they are operating procedure in an effective and efficient manner and help to ensure full compliance. Any short coming highlighted shall result in recommendations for improvement and suggestions on how to make the risk management framework more efficient and effective in line with stated objectives.
6.3	**Auditing the Risk Management Framework (refer Para 5.2 provided above):** Where there is a formal risk management framework in place, the work of the Internal Auditor shall be directed to ensure that the organisation has, amongst others: Designed the framework consistent with best-in-class and

	globally recognized frameworks, such as, COSO or ISO 31000, etc.; Implemented various enabling mechanisms, such as: Issued risk management policies and implemented supporting procedures; Set the right culture with supporting messages and activities; Designed risk management structure, established a risk management committee, appointed risk officers and assigned each risk to a specific "risk owner"; Identified all risks applicable to the entity (created a database), assessed each for importance and priority and undertaken appropriate mitigation steps or implement controls; Conduct training programs for risk officers and owners, covering knowledge and competency; Implemented robust risk management systems, deploying technology (where possible) to monitor their progress and track their status, to document timely mitigation steps and to allow timely escalation in case of any slippage; Continuously tracks performance against risk appetite, along with sufficient reviews and oversight mechanisms; Established timely communication and periodic reporting systems and protocols The Internal Auditor will review the risk management system and processes in place to evaluate whether they are operating in an effective and efficient manner and help to ensure full compliance. Any shortcoming highlighted shall result in recommendations for improvement and suggestions on how to make the risk management framework more efficient and effective in line with stated objectives.
6.4	**Auditing Risk Management Activities and Processes (refer Para 5.3 provided above):** Where management has not implemented a formal risk management framework, the Internal Auditor will conduct audit procedures over various risk management related activities which may be present (similar to those indicated under Para 3.3). These activities may be supported by certain enabling mechanisms (similar to those indicated under Para 6.3 (b)) and

	which may be recommended as desirable actions to be undertaken to establish a formal frame work.
6.5	Independent Assurance over Risk Management (refer Para 5.4 provided above): Where a written assurance report is being issued, the Internal Auditor shall also consider the following as a basis for audit opinion: (a) The linkage of the risk management framework with the system of CEO and CFO certification on Internal Controls; and (b) Certificates of self-compliance from owners of key risks to support a system of continuous compliance.

Fraud Risk Management

As all are aware of, "Fraud" is wrong full or criminal perception to result in financial gain of those committing fraud at the cost of any person or entity/ organisation. It is essential for NBFC, being an organisation **for managing its risk**, to ensure that its employees are aware of what constitutes a fraud, how they should avoid such acts, stay alert and bring to the notice of the management any deviations that can be construed as fraudulent to the appropriate authority. The management to ensure in-built systems to detect frauds. Once detected, it is ensured that measures to gather evidence against the perpetrators of the fraud is established.

Fraud Detection and Fraud Deterrence

Each organization has its own established value systems and, therefore, would like its employees to follow a code of conduct. This provides the management a medium to interact with employees in defining the ground rules to be followed and actions that are not acceptable. For the purpose, management must define what types of conduct may involve conflict of interest (or potential for a conflict of interest) vis- à-vis the official duties. This may or may not involve any pecuniary interest and may extend to any bias towards third persons in the official dealings/ decisions. Hence, non-competitive pricing of products or unjustified commercial dealings could be within the purview of this code of conduct.

Generally, employees are the first point of contact in noticing a fraudulent activity arising out of certain unusual or abnormal practices. These remain unreported to the superior reporting officer due to lack of training and awareness among the employees. The insecurity among employees is another reason for not escalating the matter to the reporting authority.

Therefore, employees to be made aware of their role in detection as well as deterrence to such fraudulent acts and apprise them of the reporting process through appropriate mediums.

Apart from providing abundant opportunity to the employees within the organization to stay away from fraudulent acts and to report any such deceit to the appropriate authority, it is essential to set up independent monitoring system or devise strategies which work coherently with the following objectives:

- Identification and reporting of unusual activities;
- Isolating deviations and surveillance mechanism in the day- to-day operations;
- Use of computer applications and audit tools in keeping track of unusual transactions;
- A robust accounting and management information reporting system; and
- Effective interaction with the Chief Internal Auditor for appropriate audit reviews.

It is preferable that there should be an effective incident reporting process normally to a designated official (heading the investigative cell or compliance officer) to whom all the suspected activities will be reported. It should be his responsibility to promptly update the management of such incident**.**

The senior management executives need to consistently make an effort of educating the employees and related third parties on how to be alert to fraudulent activities, including suspicious activities and the manner in which the same needs to be communicated. In addition, the internal audit observations can be filtered to identify red flags and used as a medium to apprise employees of internal control gaps in prevention or detection of frauds.

When a fraud is suspected, certain immediate steps may need to be taken to prevent loss of evidence or furtherance of such acts. For the purpose, records and documents are taken in safe custody and the persons connected with the activities are generally transferred to other activities till the perpetrator of the fraud is identified. The scope and period of coverage is dependent on judgement and this in turn would determine the time required to complete the assessment process.

These may relate more to the activities impacted due to fraud including fraudsters' access to records, documents and information. Unravelling the

modus operandi of the fraudulent act could be equally complex with reference to identifying and deciphering the trail left by the fraudster and in gathering requisite evidence. This is followed by an assessment of damages arising out of the wrongful act. In case the entity has an insurance cover, the insurer is informed of the incident and thereafter the extent of damages is notified. The management has the option of either proceeding with legal action or can take disciplinary action on the erring employee or third party if the situation warrants. Where the perpetrator is not known steps may be taken for in-depth investigation either by in- house resource or external agencies.

Initiating Investigative Process

Once a fraud is reported, a preliminary investigation to be conducted first to assess and verify the enormity of the act and then the next step is to substantiate it with evidence. It is preferred that this is carried out under the aegis of generally, a Chief Financial Officer in full time employment with the company.

The Compliance Officer, generally, a person of integrity and based on his past track record, have the ability to manage situations of fraud risk. He is, normally, a person who is trusted by the management in safeguarding the reputation and image of the organization.

To achieve this objective, a Compliance Officer is an official who by the nature of his duties, generally, reports to the senior most officer in the company (CEO or Managing Director). The Compliance Officer may seek the support of the internal auditor in discharging his duties on matters relating to the investigation.

All organisations generally have a fraud control unit (FCU) who assists the management in conducting the preliminary assessment of each situation and depending upon the magnitude of suspected fraud (which is by and large a matter of subjective judgment) will decide whether they have the resources within the organization to carry out a full-fledged investigation and the extent of outsourcing of the investigative activities.

FCU role and responsibility may include the following:

- Interaction with the internal auditor of the company.
- Resource mobilization, either internally or outsourced for conducting investigation.
- Sequencing of the events and activities for diagnosis of the problem.

- Internal control assessment in highlighting vulnerabilities.
- Preliminary assessment on the role of internal and external persons who are suspected to be involved in the alleged irregularities and details thereof.
- Damage assessment arising out of the reported incident.
- Collation of information on suspected fraudulent activity.
- Ensuring a reporting format to the senior management or regulators such as RBI, IRDA, SEBI, NHB, etc.
- Comment on available evidence to form an opinion.

Considering the sensitivities involved in any information that relates to a fraudulent activity, it is essential that adequate confidentiality is ensured in collating such information and reporting. Based on his report management can form an opinion on the future course of action including referral for legal action, reporting to police authorities, filing of insurance claims, disciplinary action against delinquent employees, etc.

Managing Risk

The role of an FCU / investigating person/authority is different from that of the line functionaries, as his primary concern would be to corroborate facts based on available evidence, within the legal realms. Senior executives must give a free hand to the investigating officer and should not intrude into their investigative approach and methodology. Such intrusion tends to be counterproductive. The desired course of management action will depend on the regular updates on the progress made in the investigation. It may be noted that just as the senior management is responsible for initiating the investigation, they have a similar right to call off an investigation.

Post discovery of a fraudulent activity, the manner in which the enquiry process is conducted may be defined through a policy document. This will include the options available for disciplinary actions that could be explored by the management.

Anti-fraud programs enable the management to identify areas that are vulnerable to potentially fraudulent activities. Where such events are inherent to the business environment, counter measures for identification of irregularities and timely action should be ensured.

Unless warranted by law or regulatory institutions such as, Reserve Bank of India norms, it is the management's discretion as to whether an incident

needs to be reported to the police authorities. A weak or inadmissible evidence or reputation risk to the organization is sometimes a reason for not proceeding legally against the erring employees.

The management to ensure that the above incidents are brought to the notice of the Chief Internal Auditor in a timely manner, including management action plan and corrective steps, to be taken post discovery of the fraud. There should be a standard format in which the management informs the audit committee and the board about the status of frauds reported, persons involved, types of fraud, recoveries, corrective measures and regular updates on investigations in progress.

Internal Audit of Information Security

5.15 Information security in an NBFC is of paramount importance to protect sensitive data, maintain trust with customers, and ensure regulatory compliance. NBFCs, like other financial institutions, handle a significant amount of confidential and financial information, making them attractive targets for cyberattacks and data breaches.

Standard on Internal Audit (SIA) 520, Internal Auditing in an Information Technology Environment and Standard on Internal Audit (SIA) 530, Third Party Service Provider as issued by the ICAI explains that An Information Technology Environment (ITE) exists when information is captured, stored and processed through automated means and is managed through various policies and procedures to support business operations and objectives

Information is a critical asset to a company and Information Security ("IS") refers to the protection of these assets to achieve the company's financial and operational goals.

The purpose of Information Security is to monitor and control the access to sensitive information that resides with the organisation, ensuring use only by legitimate users so that data and information cannot be read or compromised by unauthorized access. In the same way, the Communication inward and outward is to follow the Company's protocol, rules & regulations and only those authorised-on behalf of the Company need to communicate within a set guideline. This is primarily driven by four tenets:

Confidentiality – Ensuring that unauthorized access to sensitive data is prohibited.

Integrity – Ensuring accuracy, completeness, and consistency of data & information by ensuring that it is stored in the best feasible way and does not change when modified, transferred, or accidentally deleted.

Availability – Ensuring that uninterrupted data is available at a required level of performance to users in situations ranging from normal to disastrous.

Authenticity – Ensuring that authenticity of data is maintained while processing or analysis of data.

Accordingly, the NBFC should:

- Establish a strong Information Security Governance structure.
- Monitor and proactively protect the infrastructure of all departments within the organisation.
- Deploy security controls to safeguard resources from disruption, modification, and disclosure.
- Provide Information Security awareness and education for employees and vendors.
- Foster a security-conscious culture within the organization.
- Comply with legal, regulatory, and contractual requirements.
- Regularly test and maintain business continuity and incident response plans.
- Conduct risk management to identify and implement appropriate controls.
- All employees of the organisation must comply with the policies, with non-compliance leading to appropriate action.
- Maintain information and information processing resources based on a need-to-know and need-to-access basis, protecting against unauthorized use.
- Establish an Information Security Policy aligned with business practices.

Role of the Management

Physical Security: Implementing security measures to restrict access to data centres, server rooms, and other critical physical locations. Using surveillance systems to monitor and record access to sensitive areas.

Network Security: Deploying firewalls to control incoming and outgoing network traffic and using intrusion detection/prevention systems to identify and mitigate potential threats. Implementing secure network designs and segmentation to isolate sensitive data from public-facing systems.

Access Control: Implementing strong authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity of users accessing

systems and data. Assigning access permissions based on job roles and responsibilities to ensure that employees only have access to the data and systems necessary for their work.

Data Protection: Identifying and categorizing data based on its sensitivity and criticality to determine appropriate security measures. Encrypting sensitive data both in transit and at rest to protect it from unauthorized access.

Incident Response: Establishing procedures for employees to report security incidents promptly. Developing a well-defined incident response plan to address security breaches and minimize their impact.

Vulnerability Management: Conducting vulnerability assessments and promptly applying security patches and updates to mitigate known vulnerabilities.

Security Awareness and Training: Educating employees about cybersecurity best practices, social engineering threats, and their role in maintaining security. Training employees to recognize and report phishing attempts and other social engineering attacks.

Regulatory Compliance: Ensuring compliance with relevant data protection and financial regulations, such as the Information Technology Act, RBI Guidelines, General Data Protection Regulation (GDPR) and data localization requirements, as applicable.

Vendor Management (incl. Outsourcing Management): Assessing and monitoring the security practices of third-party vendors and service providers that have access to NBFC data.

Business Continuity and Disaster Recovery: Developing and testing business continuity and disaster recovery plans to ensure data and operations can be restored in the event of a disruption or disaster.

Information System Audit

- IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications, etc.
- Refer to guidance issued by Professional bodies like ISACA, IIA, ICAI for issuance of IS Audit framework Should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up.
- Evaluate the effectiveness of business continuity planning, disaster recovery set up.

- IS audit should be undertaken preferably prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

Role of Internal Audit

It is paramount that Information Systems audit is conducted on a timely basis by an expert. The audit planning and execution should take into account following:

- Agreeing on audit scope and objectives with Senior Management and place the audit plan before the IT Strategy Committee for any directional views.
- Conducting the assessment in a controlled environment Wherever possible, read-only access to software and data to be given for conducting the audit.
- All audit activities shall be logged to provide documented details about the tasks performed, audit procedures, findings, and recommendations.
- The users shall participate in investigations of suspected information security misuse or in compliance reviews as requested by auditors.
- Technical compliance check shall be conducted to identify the vulnerabilities in the system and to check the effectiveness of the controls to prevent unauthorized access to the information systems.
- Information systems shall be checked at regular intervals for their compliance with the security policies and procedures.
- To ensure technical compliance, the organisation should follow a calendar defining frequency of vulnerability assessments and penetration testing as defined in Cyber Security policy.
- Any technical compliance review shall only be conducted by competent, authorized persons or under the supervision of such persons It shall be communicated to all employees, third party users and contractors that compliance to organization's security policy is mandatory.
- An agreement shall be signed by all employees, agreeing to abide by the organization's information security policy. This shall be made a part of recruitment process.

- There shall be a regular review of compliance vis-à-vis the information security policies. Any deviations shall be noted and communicated to the management as a part of the Internal Audit Report.
- The CIO shall ensure that all observations are addressed in the agreed timeframes.
- If any non-compliance is found because of the review, managers shall:
    - Identify the causes of the non-compliance.
    - Evaluate the need for actions to achieve compliance.
    - Implement appropriate corrective action.
    - Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.
    - Results of reviews and corrective actions conducted by managers shall be recorded and these records shall be maintained. Managers shall report the results to the persons conducting independent reviews (Ref: independent review of information security) when an independent review takes place in their responsibility.
- If audit tool is being used to conduct the internal audit:
    - The original copy of the audit tool shall be stored on a non-rewritable medium.
    - Copies of the audit tool software shall not be allowed to be stored on desktops and/or servers.
    - If during the process of a system audit, a software agent needs to be deployed on a system, the same shall be removed / uninstalled completely at the end of the audit run.
    - Formal authorization shall be obtained from CISO and Head - Technology before installing audit tool on any system.
    - Reports generated using audit tools shall be strictly controlled and access to such reports shall be only based on need-to-know and need-to-do basis.

Convergence between Head of Internal Audit (HoIA), Chief Compliance Officer (CCO), Chief Risk Officer (CRO) and Chief Information Security Officer (CISO) and Expectations from the Regulator

5.17 The even changing landscape of corporate governance, risk management, and information security has led to a significant transformation and expectation in the roles and responsibilities of key executives within organizations.

CCO, CRO, CISO and HoIA are considered four pillars of Assurance function within the organisation, who are expected to steer the organisation in right direction in an ethical way.

These areas are interconnected and inter dependent as well. Though Internal Audit is considered more independent than other 3 assurance functions, it cannot operate in isolation.

Regulators around the world are acknowledging this trend and have specific expectations from organizations in integrating these functions to enhance overall governance, risk management, and security.

CCO: The Chief Compliance Officer (CCO) plays a pivotal role in an organization by ensuring that the organisation's operations and activities comply with relevant laws, regulations, industry standards, and internal policies. The primary function of a CCO is to establish and maintain a robust compliance program that helps the organization operate within legal and ethical boundaries.

CRO: The Chief Risk Officer (CRO) is responsible for overseeing and managing organization's risk management framework. The primary function of a CRO is to identify, assess, monitor, and mitigate risks that could affect the organization's operations, financial stability, reputation, and objectives.

CISO: The Chief Information Security Officer (CISO) is responsible for overseeing organization's information security program. The CISO's main functions revolve around protecting the organization's sensitive data, information systems, and technology infrastructure from cybersecurity threats and ensuring compliance with relevant regulations.

HoIA: The Head of Internal Audit (HoIA) plays a crucial role in an organization's governance and risk management by providing independent and objective assessments of its internal controls, processes, and operations.

Regulators are increasingly recognizing that these functions should not operate in isolation. They expect organizations to foster collaboration and convergence among the HoIA, CCO, CRO, and CISO.

By working together, these roles can identify emerging risks more effectively, allowing the organization to take proactive measures rather than being reactive.

Regulators appreciate that convergence helps organizations maintain compliance with evolving regulations and standards. It reduces the likelihood of compliance gaps and improves reporting accuracy.

With the increasing prevalence of cyber threats, regulators are keen on seeing information security seamlessly integrated into risk management practices. A unified approach is critical for maintaining cybersecurity resilience.

Regulators understand that risks are interconnected. An event that starts as an information security breach can have cascading effects on compliance, operational efficiency, and financial stability. Convergence allows for a more holistic approach to risk management.

Lastly, collaboration and sharing of information between these functions can lead to streamlined processes, better allocation of resources, and a more effective response to risks and regulatory requirement.

Chapter 6
Keeping NBFCs Resilient from Shocks

Regulators Initiative

6.1 In recent times, the Reserve Bank of India (RBI) has made significant strides in fortifying its regulatory and supervisory framework for banks and other regulated entities. The RBI's approach revolves around reinforcing the financial sector's ability to withstand shocks and tumultuous situations, ultimately ensuring that these entities continue to contribute to the nation's economic development.

Systemic resilience hinges on both the individual strength of financial institutions and the connections between them. To create a future-ready NBFC that is resilient, it must exhibit financial, operational, and organizational resilience. Financially, an NBFC should possess ample capital reserves and the capacity to generate earnings even in the face of severe economic upheavals. Equally important is maintaining adequate liquidity to meet obligations in diverse scenarios. Financial resilience is intricately linked to an NBFC's business model and strategy. Recognizing this, the RBI has initiated closer scrutiny of NBFC business models. Beyond mere regulatory norms for capital adequacy and liquidity ratios, the RBI is encouraging NBFCs to bolster capital reserves during prosperous periods.

The RBI has introduced several prudential regulatory frameworks, including capital adequacy requirements, asset classification, provisioning guidelines, dividend distribution criteria, and liquidity management frameworks. Periodically, it is seen that the RBI employs macro-prudential measures to address systemic risks.

Further recognizing the growing reliance on third-party technology and IT-enabled services, the RBI issued comprehensive guidelines on Information Technology outsourcing on April 10, 2023, which apply to banks, NBFCs, and other regulated entities. The third facet of resilience lies in being organizationally resilient. This means early risk anticipation and efficient absorption of risks. Organizations should have the capacity and flexibility to protect themselves from adverse incidents and safeguard their balance

sheets. Achieving organizational resilience involves standardizing policies, processes, organizational culture, and governance. It should also foster an environment that encourages diverse ideas and innovations within the organization.

The Pillars of the Reserve Bank's Regulatory and Supervisory Strategy rests on three pillars:

Strengthening Governance and Assurance Functions: Effective governance is crucial for ensuring the safety and soundness of the NBFC sector. It fosters trust, transparency, and accountability. To achieve this, regulated entities should implement systems and processes that promote sound corporate governance. Assurance functions, such as risk management, compliance, and internal audits, bridge the gap between governance and business operations. The RBI has issued comprehensive guidelines to ensure the quality and independence of governance and assurance functions. These areas are subject to rigorous supervisory assessments.

Regulatory Initiatives: The RBI has introduced several regulatory initiatives to strengthen governance, risk management, audit, and compliance functions. These encompass scale-based regulatory frameworks, guidelines for the appointment of Chief Risk Officers (CROs) for NBFCs with assets exceeding ₹5,000 crores with specified roles and responsibilities, thereby enhancing risk management and Chief Compliance Officers (CCOs) in large NBFCs, liquidity coverage ratios, risk-based internal audit norms, and harmonized guidelines for the appointment of statutory auditors. The inclusion of Housing Finance Companies (HFCs) under the RBI's regulatory purview is significant, considering their asset-liability profiles have been some of the key initiatives by RBI.

The Significance of Effective Audits: To earn the trust of both current and prospective customers, NBFCs require a robust assurance mechanism through internal audits. This mechanism provides independent evaluation and assurance that operations adhere to prescribed policies and procedures. Statutory auditors also play a critical role in maintaining market confidence in audited financial statements. The quality of audits is essential to this public role, and the RBI closely monitors the performance of statutory auditors in regulated entities.

Emerging Trends and Impact of Technology

6.2 The NBFCs sector has witnessed a huge surge of technological revolution some of these are listed below.

Artificial Intelligence (AI) and Machine Learning (ML) – Driven Predictive Financing

Artificial Intelligence has brought about a big beneficial change in the financing industry as with its help they can now consolidate all internal and external data, build predictive profiles of customers and members in real time. Thus, with a consumer data that is rich, accessible and financially viable to deploy, the non-banking financial institutions are not only able to know their customers, but also provide advice for the future.

Hence Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing risk assessment and underwriting processes. NBFCs are using AI algorithms to analyse vast sets of data, enabling more accurate credit decisions. Additionally, ML helps in detecting fraudulent activities and managing credit risk.

Voice & Vernacular – The Next Frontier: In the list of upcoming trends applications-voice in digital payments will play an important role, as it will be further enabled by different Indian languages. This will help the NBFCs in a big way in reaching the next set of users who are new to the internet and Voice will certainly make experiences more interactive and help reach the masses.

Video KYC – A Great Enabler: Video KYC is a feature that is aimed to become the future of identity verification as no other solution has come this close to eliminating identity fraud online.

Cloud Integration – Bringing in Ease and Efficiency: Cloud computing has helped NBFCs in creating a flexible business model that fulfils growing business needs. Some of the prominent advantages of cloud services are lower costs, quick implementation, and near-universal availability.

Automation – Actualizing Speedy Outcomes: Another important future innovation which has strongly impacted the functioning of NBFCs is the power of Automation. It is a technology that is helping in speeding up the lending processes and facilitates consistency in decisions.

Chatbots & Robo-Advisors: Some of the NBFCs have already employed chatbots and robo-advisors that interact with prospects and customers for

self-onboarding of the customer, customer servicing and employee-related services. Most of these chatbots and robo-advisors have been developed with vernacular capabilities, making them well-suited for rural and semi-urban India and thus, the entire process of availing various financial services by masses has become much easier and hassle-free.

Biometrics – Fingerprint, Face & Iris Recognition: Through biometric-based authentication, the NBFCs is able to uniquely identify an individual by evaluating one or more of his/her distinguishing biological traits- like their fingerprints, voice waves, or retina and iris patterns. For customer's KYC authentication, the financial entities use either the fingerprints or iris patterns of an individual to authenticate their identities.

Peer-to-Peer (P2P) Lending: P2P lending platforms have gained popularity, allowing individuals to lend and borrow money directly from each other, circumventing traditional financial intermediaries. NBFCs are recognizing the potential of P2P lending as an alternative investment avenue and are participating as lenders on these platforms.

Mobile Banking and Apps: Mobile banking apps and digital wallets are becoming central to NBFCs' customer engagement strategies. These apps enable customers to access their accounts, make transactions, and apply for loans conveniently, enhancing accessibility and customer satisfaction.

Alternative credit scoring: The game changer: The non-traditional sources of data, coupled with advanced analytics, is been used by many NBFC's to assess the creditworthiness of large and previously untapped customer

Impact on Financial Inclusion: The adoption of technology has positively impacted financial inclusion. NBFCs are extending their services to underserved areas and populations, thanks to the ease of digital operations. By leveraging innovative technologies, they can offer financial products to a more extensive customer base, helping bridge the financial gap

Future Outlook of NBFC Sector

6.3 The transformation of NBFCs in the pursuit of a more resilient, efficient, and trusted financial system is both inevitable and desirable because of the unstoppable process of change triggered by the winds stemming from market risk, technology, consumer protection and sustainability. The transformation of the form and substance of NBFCs in India is a tall order and necessitates synchronized efforts by all stakeholders

with a sense of urgency. With strong capital buffers, adequate provisions, and sufficient liquidity in their books promises well for the NBFCs.

Given the winds of change sweeping the globe, we see an accent on digitization, including chatbots to enhance customer service, provide digital solutions, and develop alliance with fin-techs as partners in development. With increasing use of instruments such as, eKYC (Electronic Know Your Customer), e-signature, and Aadhaar-based verification, NBFCs are driving financial inclusion, increasing penetration of financial assets, wider participation in equity markets and technology adoption.

The Reserve Bank of India (RBI) significant strides in stimulating its regulatory and supervisory framework for NBFC sector there has been a spike in annual cancellations of NBFCs by the RBI occurs largely because of flawed lending practices and the widespread tendency to adopt short-term ad hoc measures. RBI also proposed a scale-based regulatory framework for NBFCs to promote better governance and structural strengthening of the sector, with the long-term objective of bridging the gap between banks and NBFCs. These regulations mark a paradigm shift from an activity-based regulation to one based on riskiness and scale of operations, following the principle of proportionality. These measures together with application of other regulatory prescriptions, such as, PCA and IRACP (Income Recognition, Asset Classification and Provisioning) norms would strengthen the NBFCs and make them more robust and scalable over the medium-term.

NBFCs sector has a promising growth by increasingly using digital solutions, flexible underwriting practices and leveraging data analytics. With India's 'Atmanirbhar Bharat' move going full steam ahead and the pursuit of US$ 5 trillion target by 2025, the NBFCs can help to plug the gaps in the lending eco-system.

(Source: Industry Outlook: NBFCs and The Travails of Transition as issued by INFOMERICS Valuation and Rating Private Limited that is a SEBI registered and RBI accredited Credit Rating Agency.)

Reference

Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs	https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12179&Mode=0
Risk Based Internal Audit in NBFCs	https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12018&Mode=0
Guidance note on Risk Based Internal Audit in Banks issued by Reserve Bank of India	https://rbidocs.rbi.org.in/rdocs/notification/PDFs/33472.pdf
Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on January 04, 2024)	https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607
RBI directions on Managing risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Companies	https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=2646
Master Direction on Outsourcing of Information Technology Services	https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486
Guidelines on Default Loss Guarantee (DLG) in Digital Lending	https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12514&Mode=0
Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016	https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10622
Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023	https://rbidocs.rbi.org.in/rdocs/content/pdfs/106MDNBFCs191020 23_ANN.pdf
Master Direction – Reserve Bank of India (Securitisation of Standard	https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=

Assets) Directions, 2021 (Updated as on December 05, 2022)	12165
RBI directions on Managing risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Companies	https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=2646
Recommendations of the Working group on Digital Lending - Implementation	https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54187
Guidelines on Default Loss Guarantee (DLG) in Digital Lending	https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12514&Mode=0#AN
Industry Outlook: NBFCs and The Travails of Transition as issued by INFOMERICS Valuation and Rating Private Limited	https://www.infomerics.com/admin/uploads/nbfc-outlook-mar23.pdf