भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/422
DoS.CO.PPG.16/11.01.005/2026-27 July 31, 2026

Reserve Bank of India (Small Finance Banks - Internal Audit Function) Directions, 2026 (Updated as on October 1, 2026)

Table of Contents

Introduction 3

Chapter I - Preliminary 3

A. Short Title and Commencement 3

B. Applicability 3

C. Definitions 3

Chapter II - Governance and Oversight 4

A. Role of the Board 4

B. Role of the Senior Management 5

Chapter III - Risk-Based Internal Audit Framework 6

A. Policy on Internal Audit 6

B. Functional Independence 6

C. Risk Assessment 7

D. Scope 11

E. Communication 12

F. Performance Evaluation 13

G. Outsourcing 13

Chapter IV - Head of Internal Audit 15

A. Authority, Stature, and Independence 15

B. Tenure 15

C. Reporting Line 15

Chapter V - Repeal and Other Provisions 16

A. Repeal and Saving 16

B. Application of Other Laws Not barred 16

पर्यवेक्षण विभाग, भारतीय रिज़र्व बैंक, केंद्रीय कार्यालय, मेकर टावर-ई, 20वीं मंजिल, कफ परेड, कोलाबा, मुंबई-400 005
दूरभाष: 022-6997 3798 ई-मेल: ppgdos@rbi.org.in

Department of Supervision, Reserve Bank of India, Central Office, Maker Tower-E, 20th floor, Cuffe Parade, Colaba, Mumbai- 400 005
Tel: 022- 6997 3798 Email: ppgdos@rbi.org.in

हिंदी आसान है, इसका प्रयोग बढ़ाइए

C. Interpretations..... 17

Introduction

A sound Internal Audit function is an integral component of a bank's internal control and risk management framework. In view of the limitations of a transaction-centric audit approach, the bank is required to adopt Risk Based Internal Audit (RBIA), which places emphasis on the assessment of risk management systems and internal controls, in addition to selective transaction testing, in alignment with evolving governance standards and international best practices.

In exercise of the powers conferred by Section 35-A of the Banking Regulation Act, 1949, and all other provisions / laws enabling the Reserve Bank of India ('RBI') in this regard, RBI being satisfied that it is necessary and expedient in the public interest so to do, hereby, issues the Directions hereinafter specified.

Chapter I - Preliminary

A. Short Title and Commencement

1. These Directions shall be called the Reserve Bank of India (Small Finance Banks - Internal Audit Function) Directions, 2026.

2. These Directions shall come into effect immediately upon issuance.

B. Applicability

3. These Directions shall be applicable to Small Finance Banks (hereinafter collectively referred to as 'banks' and individually as a 'bank').

C. Definitions

4. All expressions used in these Directions, shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, the Companies Act, 2013, or any statutory modification or re-enactment thereto or other regulations issued by RBI or the Glossary of Terms published by RBI or as used in commercial parlance, as the case may be.

Chapter II - Governance and Oversight

A. Role of the Board

5. The Board of the bank shall approve the following:

   (1) A well-defined policy for undertaking RBIA.

   (2) A risk assessment methodology devised by the Internal Audit Department (IAD) of the bank, keeping in view the size and complexity of the business undertaken by the bank.

   (3) An Annual Audit Plan (AAP) which should include the schedule and the rationale for audit work planned.

   (4) A policy to engage the services of the bank's retired personnel for a maximum tenure not exceeding three years in areas where it does not have enough expertise which shall, inter alia, include the terms of engagement, review of performance, termination of services.

   Provided that for sub-paragraph (2) and (3) above, the Board may delegate the responsibility to the Audit Committee of the Board (ACB).[#]

6. The Board shall be responsible for ensuring that an effective RBIA system is in place, and its importance is understood throughout the bank.

7. The Board / Audit Committee of the Board (ACB) shall periodically assess the performance of the RBIA for reliability, accuracy, and objectivity.

8. The Board shall prescribe a minimum period of service for staff in the Internal Audit function, except for banks where the Internal Audit function is a specialised function and managed by career internal auditors. The Board may also examine the feasibility of prescribing at least one stint of service in the Internal Audit function for those staff possessing specialised knowledge useful for the audit

[#] Substituted w.e.f. October 1, 2026, consequent to Reserve Bank of India (Small Finance Banks - Governance) Amendment Directions, 2026

function, but who are posted in other departments, so as to have adequate skills for the staff in the Internal Audit function.

B. Role of the Senior Management

9. The Senior Management shall ensure that the importance of an effective RBIA system is understood throughout the bank, and the Internal Audit staff perform their duties with objectivity and impartiality.

Chapter III - Risk-Based Internal Audit Framework

A. Policy on Internal Audit

10. The primary focus of Risk-Based Internal Audit (RBIA) shall be to provide reasonable assurance to the Board and senior management about the adequacy and effectiveness of the risk management and control framework in the bank's operations. While examining the effectiveness of control framework, the RBIA shall report on proper recording as well as reporting of major exceptions and excesses.

11. The RBIA should focus on risk identification, prioritisation of audit areas, and allocation of audit resources in accordance with the risk assessment. The policy shall include the risk assessment methodology for identifying the risk areas based on which the audit plan would be formulated. It shall also lay down the maximum time period beyond which even the low-risk business activities / locations shall not remain unaudited.

12. The bank shall ensure and demonstrate through proper documentation that its RBIA framework captures all the significant criteria / principles suited for its organisational structure, business model and risks. The Information Systems Audit should also be carried out using the risk-based approach.

B. Functional Independence

13. The IAD of the bank shall be independent from the internal control process in order to avoid any conflict of interest and should be given an appropriate standing within a bank to carry out its assignments. It shall not be assigned the responsibility of performing other accounting or operational functions.

14. The bank shall distinguish between the functions of the Risk Management Department and the role of RBIA. While the Risk Management Department focuses on areas such as identification, monitoring and measurement of risks, development of policies and procedures, and use of risk management models, RBIA shall undertake an independent risk assessment solely for the purpose of formulating the risk-based audit plan keeping in view the inherent business risks

of an activity / location and the effectiveness of the control systems for monitoring the inherent risks of the business activity. While formulating the audit plan, every activity / location of the bank, including the Risk Management function, shall be subjected to risk assessment by the RBIA.

15. The bank shall provide appropriate resources and staff to the IAD to achieve its objectives under the RBIA system. Requisite professional competence, knowledge, and experience of each internal auditor are essential for the effectiveness of a bank's Internal Audit function. They should also be trained periodically to enable them to understand the bank's business activities, operating procedures, risk management and control systems, and Management Information System (MIS). The desired areas of knowledge and experience may include banking operations, accounting, information technology, data analytics, and forensic investigation, among others. The bank shall ensure that its Internal Audit function has the requisite skills to audit all areas of the bank.

16. The bank shall not link the remuneration of Internal Audit staff to the financial performance of the business lines for which they exercise audit responsibilities. The bank shall structure the remuneration policy in a way that it avoids creating conflict of interest and compromising audit's independence and objectivity.

C. Risk Assessment

17. The risk assessment should, as an independent activity, cover risks at various levels (corporate and branch; the portfolio and individual transactions, etc.) as also the processes in place to identify, measure, monitor, and control the risks.

18. The Board - approved risk assessment methodology shall, inter alia, include the following:

    (1) Identification of inherent business risks in various activities undertaken by the bank.

    (2) Evaluation of the effectiveness of the control systems for monitoring the inherent risks of the business activities ('Control risk').

(3) Drawing up a risk-matrix for considering both the factors viz., inherent business risks and control risks. An illustrative risk-matrix and guidance are given as a box item below:

Risk Matrix

Inherent Business Risks				
	High	A High Risk	B Very High Risk	C Extremely High Risk
	Medium	D Medium Risk	E High Risk	F Very High Risk
	Low	G Low Risk	H Medium Risk	I High Risk
		Low	**Medium**	**High**
		Control Risks		

Inherent business risks indicate the intrinsic risk in a particular area / activity of the bank and could be grouped into low, medium and high categories depending on the severity of risk.

Control risks arise out of inadequate control systems, deficiencies / gaps and / or likely failures in the existing control processes. The control risks could also be classified into low, medium, and high categories.

In the overall risk assessment both the inherent business risks and control risks should be factored in. The overall risk assessment as reflected in each cell of the risk matrix is explained below:

A - High Risk: Although the control risk is low, this is a High Risk area due to high inherent business risks.

B - Very High Risk: The high inherent business risk coupled with medium control risk makes this a Very High Risk area.

C - Extremely High Risk: Both the inherent business risk and control risk are high which makes this an Extremely High Risk area. This area would require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring

by the bank's top management.

D - Medium Risk: Although the control risk is low, this is a Medium Risk area due to medium inherent business risks.

E - High Risk: Although the inherent business risk is medium, this is a High Risk area because of control risk also being medium.

F - Very High Risk: Although the inherent business risk is medium, this is a Very High Risk area due to high control risk.

G - Low Risk: Both the inherent business risk and control risk are low.

H - Medium Risk: The inherent business risk is low, and the control risk is medium.

I - High Risk: Although the inherent business risk is low, due to high control risk this becomes a High Risk area.

The bank should also analyse the inherent business risks and control risks with a view to assess whether these are showing a stable, increasing or decreasing trend. Illustratively, if an area falls within cell 'B' or 'F' of the Risk Matrix and the risks are showing an increasing trend, this will also require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring by the bank's top management (as applicable for cell 'C'). The Risk Matrix shall be prepared for each business activity / location.

Transaction testing shall be an essential aspect of RBIA. The extent of transaction testing shall be determined based on the risk assessment. Illustratively, the bank shall undertake 100 per cent transaction testing if an area falls in cell 'C-Extremely High Risk' of the risk matrix. The bank may also consider 100 per cent transaction testing if an area falls in cell 'B-Very High Risk' or 'F-Very High Risk, and the risks are showing an increasing trend. The bank may also consider transaction testing with an element of surprise in respect of low risk areas which are audited at relatively longer intervals.

19. The basis for determination of the level (high, medium, low) and trend (increasing, stable, decreasing) of inherent business risks and control risks should be clearly spelt out. The risk assessment may make use of both quantitative and qualitative approaches. While the quantum of credit, market, and

operational risks could largely be determined by quantitative assessment, the qualitative approach may be adopted for assessing the quality of controls in various business activities.

20. In order to focus attention on areas of greater risk to a bank, an activity-wise and location-wise identification of risk should be undertaken.

21. The bank shall put in place an independent risk assessment system in the IAD for focusing on the material risk areas and prioritising the audit work. The methodology may range from a simple analysis of why certain areas should be audited more frequently than others in the case of small sized banks undertaking traditional banking business, to more sophisticated assessment systems in large sized banks undertaking complex business activities.

22. The risk assessment methodology should, inter alia, cover the following parameters:

    (1) Previous internal audit reports and compliance

    (2) Proposed changes in business lines or change in focus

    (3) Significant change in management / key personnel

    (4) Results of latest regulatory examination report

    (5) Reports of external auditors

    (6) Industry trends and other environmental factors

    (7) Time elapsed since last audit

    (8) Volume of business and complexity of activities

    (9) Substantial performance variations from the budget

23. For the risk assessment to be accurate, a bank shall have proper MIS and data integrity in place. The Internal Audit function should be kept informed of all developments, including introduction of new products, changes in reporting lines, and changes in accounting practices / policies. The risk assessment should

invariably be undertaken at least annually and should also be periodically updated to take into account changes in business environment, activities, and work processes.

D. Scope

24. The Board-approved AAP should include all risk areas, and their prioritisation based on the level and direction of risk. Illustratively, the areas or activities identified as high, very high or extremely high risk (based on risk matrix) may be audited at shorter intervals as compared to medium or low risk areas, which may be audited at longer intervals subject to applicable regulatory directions.

25. The bank may prepare a Risk Audit Matrix as shown below:

Risk Audit Matrix				
Magnitude of Risk (M) ↑	**High**	High Magnitude & Low Frequency	High Magnitude & Medium Frequency	High Magnitude & High Frequency
	Medium	Medium Magnitude & Low Frequency	Medium Magnitude & Medium Frequency	Medium Magnitude & High Frequency
	Low	Low Magnitude & Low Frequency	Low Magnitude & Medium Frequency	Low Magnitude & High Frequency
		Low	**Medium**	**High**
		Frequency of Risk (F) →		

26. AAP should prioritise audit work to give greater attention to the areas of:

(1) High magnitude and high frequency

(2) High magnitude and medium frequency

(3) Medium magnitude and high frequency

(4) High magnitude and low frequency

(5) Medium magnitude and medium frequency.

27. The precise scope of RBIA shall be determined by a bank for low, medium, high, very high, and extremely high risk areas. However, at the minimum, it shall review / report on:

    (1) process by which risks are identified and managed in various areas;

    (2) the control environment in various areas;

    (3) gaps, if any, in control mechanism which might lead to frauds, identification of fraud prone areas;

    (4) data integrity, reliability and integrity of MIS;

    (5) internal, regulatory and statutory compliance;

    (6) budgetary control and performance reviews;

    (7) transaction testing / verification of assets to the extent considered necessary;

    (8) monitoring compliance with the RBIA report; and

    (9) variation, if any, in the assessment of risks under the AAP vis-à-vis the RBIA.

28. The scope should also include a review of the systems in place for ensuring compliance with money laundering controls; identifying potential inherent business risks and control risks, if any; suggesting various corrective measures and undertaking follow up reviews to monitor the action taken thereon.

E. Communication

29. The bank should ensure that the communication channels between the RBIA staff and senior management encourage reporting of negative and sensitive findings. All serious deficiencies should be reported to the appropriate level of management as soon as they are identified. Significant issues posing a threat to the bank's business should be promptly brought to the notice of the Board, ACB or senior management, as appropriate.

F. Performance Evaluation

30. IAD shall conduct periodic reviews, annually or more frequently, of the RBIA undertaken by it vis-à-vis the approved AAP. The performance review should also include an evaluation of the effectiveness of RBIA in mitigating identified risks.

31. Variations, if any, in the risk profile as revealed by the RBIA vis-à-vis the risk profile as documented in AAP should also be looked into to evaluate the reasonableness of risk assessment methodology of the IAD.

G. Outsourcing

32. The bank shall not outsource the Internal Audit Function. However, where required, the bank can hire experts, including former employees, on contractual basis subject to the ACB being assured that such expertise does not exist within the audit function of the bank. Any conflict of interest in such matters shall be recognised and effectively addressed. The bank shall ensure that experts so engaged work under the close supervision of the management of the bank. Ownership of audit reports in all cases shall rest with regular functionaries of the Internal Audit function.

33. The bank shall, inter alia, consider the following aspects to prevent any risk of breakdown in internal controls on account of contractual arrangements with external experts:

    (1) Before entering into an outsourcing arrangement for RBIA, the bank shall perform due diligence to satisfy itself that the outsourcing vendor has the necessary expertise to undertake the contracted work. The contract, in writing, should at the minimum, specify the following:

        (i) the scope and frequency of work to be performed by the vendor;

        (ii) the manner and frequency of reporting to the bank; and the manner of determining the cost of damages arising from errors, omissions, and negligence on the part of the vendor;

(iii) the arrangements for incorporation of changes in the terms of contract, should the need arise;

(iv) the locations where the work papers will be stored;

(v) the internal audit reports are the property of the bank and that all work papers are to be provided to the bank when required;

(vi) the employees authorised by the bank are to have reasonable and timely access to the work papers; and

(vii) the supervisors are to be granted immediate and full access to related work papers.

(2) The management should continue to satisfy itself that the outsourced activity is being competently managed.

(3) All work done by the vendor should be documented and reported to the senior management through the IAD.

(4) To avoid significant operational risk that may arise on account of a sudden termination of the outsourcing arrangement, the bank shall have in place a contingency plan to mitigate any discontinuity in audit coverage.

Chapter IV - Head of Internal Audit

A. Authority, Stature, and Independence

34. The bank shall ensure that the Internal Audit function has sufficient authority, stature, independence, and resources within the bank, thereby enabling internal auditors to carry out their assignments with objectivity. The Head of Internal Audit (HIA) shall be a senior executive of the bank who shall have the ability to exercise independent judgement.

35. The HIA shall have the authority to communicate with any staff member and have access to all records or files that are necessary to carry out the entrusted responsibilities.

36. The HIA shall not have any reporting relationship with the business verticals of the bank and shall not be given any business targets.

B. Tenure

37. Except for banks where the Internal Audit function is a specialised function and managed by career internal auditors, the HIA shall be appointed for a reasonably long period, preferably for a minimum of three years.

C. Reporting Line

38. The HIA shall directly report to either the ACB / Managing Director and Chief Executive Officer (MD & CEO) or Whole Time Director (WTD). Wherever the MD & CEO or WTD is the ‘reporting authority’ of the HIA, the ‘reviewing authority’ shall be with the ACB and the ‘accepting authority’ shall be with the Board in matters of performance appraisal of the HIA. In such cases, the ACB shall meet the HIA at least once in a quarter, without the presence of senior management, including the MD & CEO / WTD.

Chapter V - Repeal and Other Provisions

A. Repeal and Saving

39. With the issue of these Directions, the existing Directions, instructions, and guidelines relating to Internal Audit Function as applicable to Small Finance Banks stand repealed, as communicated vide circular no. DoS.CO.PPG.66/11.01.005/2026-27 dated July 31, 2026. The Directions, instructions and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

40. Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed Directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions. Further, the repeal of these Directions, instructions, or guidelines shall not in any way prejudicially affect:

    (1) any right, obligation or liability acquired, accrued, or incurred thereunder;

    (2) any penalty, forfeiture, or punishment incurred in respect of any contravention committed thereunder;

    (3) any investigation, legal proceeding, or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture, or punishment as aforesaid; and any such investigation, legal proceedings or remedy may be instituted, continued, or enforced and any such penalty, forfeiture or punishment may be imposed as if those directions, instructions, or guidelines had not been repealed.

B. Application of Other Laws Not barred

41. The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or directions, for the time being in force.

C. Interpretations

42. For the purposes of giving effect to the provisions of these Directions or for removing any difficulties in their application or interpretation, RBI may, if it deems necessary, issue such clarifications as it considers appropriate in respect of any matter covered herein. The interpretation of any provision of these Directions by RBI shall be final and binding on all concerned entities.

(Tarun Singh)
Chief General Manager