भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2020-21/88
Ref.No.DoS.CO.PPG./SEC.05/11.01.005/2020-21 February 03, 2021

The Chairman / Managing Director / Chief Executive Officer
All deposit taking Non-Banking Financial Companies (NBFCs)
All non-deposit taking NBFCs (including Core Investment Companies) with asset size of ₹5,000 crore and above
All Primary (Urban) Co-operative Banks (UCBs) with asset size of ₹500 crore and above

Madam / Dear Sir,

Risk-Based Internal Audit (RBIA)

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, *inter alia,* sufficient authority, proper stature, independence, adequate resources and professional competence.

2. The range and commonality of risks faced by Supervised Entities (SEs) would warrant effective and harmonized systems and processes for the internal audit function across the SEs based on certain common guiding principles.

3. The introduction of Risk-Based Internal Audit (RBIA) system was mandated for all Scheduled Commercial Banks (except Regional Rural Banks) vide our circular DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002, which was further supplemented vide circular DoS.CO.PPG./SEC.04/11.01.005/2020-21 dated January 07, 2021. It has now been decided to mandate RBIA framework for the following Non-Banking Financial Companies (NBFCs) and Primary (Urban) Co-operative Banks (UCBs):

a. All deposit taking NBFCs, irrespective of their size;
b. All Non-deposit taking NBFCs (including Core Investment Companies) with asset size of ₹5,000 crore and above; and

पर्यवेक्षण विभाग, केन्द्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर-1, कफ परेड, कोलाबा, मुंबई - 400 005
टेलीफोन: 022- 2218 8482 फैक्स: 022-2218 0157 ई-मेल - cgmicdosco@rbi.org.in
Department of Supervision, Central Office, World Trade Centre, Centre I, Cuffe Parade, Colaba, Mumbai - 400 005
Tel: 022-2218 8482 Fax: 022-2218 0157 e-mail: cgmicdosco@rbi.org.in

c. All UCBs having asset size of ₹500 crore and above[1].

4. The Supervised Entities as indicated in Para 3 above shall implement the RBIA framework by March 31, 2022 in accordance with the Guidelines on Risk-Based Internal Audit provided in the enclosed Annex. The Guidelines are intended to enhance the efficacy of internal audit systems and processes followed by the NBFCs and UCBs.

5. Further, in order to ensure smooth transition from the existing system of internal audit to RBIA, the concerned NBFCs and UCBs may constitute a committee of senior executives with the responsibility of formulating a suitable action plan. The committee may address transitional and change management issues and should report progress periodically to the Board and senior management.

6. This circular should be placed before the Board in its next meeting. The implementation of these guidelines as per timeline specified should be done under the oversight of the Board.

Yours faithfully,

(Ajay Kumar Choudhary)
Chief General Manager-In-Charge

Encl: Annex

[1] The UCBs having asset size less than ₹500 crore, all Salary Earners UCBs, Unit UCBs and UCBs under All Inclusive Directions shall continue to be covered under the extant internal audit requirements as prescribed in Master Circular DCBR.CO.BPD.(PCB).MC.No. 3/12.05.001/2015-16 dated July 1, 2015.

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

Annex

Ref. No.DoS.CO.PPG./SEC.05 /11.01.005/2020-21 dated February 03, 2021

Guidelines on Risk-Based Internal Audit (RBIA) System for Select NBFCs and UCBs

RBI vide circular DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002, had introduced Risk-Based Internal Audit (RBIA) system in Scheduled Commercial Banks (SCBs) as part of their internal control framework, which was further supplemented vide circular DoS.CO.PPG./SEC.04/11.01.005/2020-21 dated January 07, 2021. This framework relies broadly on a well-defined policy for internal audit, functional independence with sufficient standing, effective channels of communication and adequate audit resources with sufficient professional competence.

While NBFCs (Non-Banking Financial Companies) and Primary (Urban) Cooperative Banks (UCBs) have grown in size and become systemically important, prevalence of different audit system/approaches in such entities has created certain inconsistencies, risks and gaps. As SCBs, NBFCs and UCBs face similar risks by virtue of being engaged in similar financial intermediation activities, their internal audit systems also need to broadly align while keeping in mind the principle of proportionality. Considering these aspects, the Guidelines herein prescribe the broad principles that should be followed by NBFCs and UCBs to enable them to gradually move towards an RBIA system.

A. Objectives and Scope

1. An effective Risk-Based Internal Audit (RBIA) is an audit methodology that links an organisation's overall risk management framework and provides an assurance to the Board of Directors and the Senior Management on the quality and effectiveness of the organisation’s internal controls, risk management and governance related systems and processes.

2. 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. The function is an integral part of sound corporate governance and is considered as the third line of defence.
3. Historically, the internal audit system in NBFCs/UCBs has generally been concentrating on transaction testing, testing of accuracy and reliability of accounting records and financial reports, adherence to legal and regulatory requirements, etc. However, in the changing scenario, such testing by itself might not be sufficient. Therefore, SEs will have to move towards a framework which will include, in addition to selective transaction testing, an evaluation of the risk management systems and control procedures in various areas of operations. This will also help in anticipating areas of potential risks and mitigating such risks.
4. While the Risk Management Function should focus on identification, measurement, monitoring, and management of risks, development of risk policies and procedures, use of risk management models, etc., RBIA should undertake an independent risk assessment for the purpose of formulating a risk-based audit plan which considers the inherent business risks emanating from an activity / location and the effectiveness of the control systems for monitoring such inherent risks.

Expectations on the roles and responsibilities of different functionaries for this internal audit framework are provided in the following paragraphs.

B. Board of Directors / Audit Committee of Board

1. The Board of Directors (the Board) / Audit Committee of Board (ACB) of NBFCs and the Board of UCBs are primarily responsible for overseeing the internal audit function in the organization. The RBIA policy shall be formulated with the approval of the Board and disseminated widely within the organization. The policy shall clearly document the purpose, authority, and responsibility of the internal audit activity, with a clear demarcation of the role and expectations from Risk Management Function and Risk Based Internal Audit Function. The policy should be consistent with the size and nature of the business undertaken, the complexity of operations and should factor in the key attributes of internal audit function relating to independence, objectivity, professional ethics, accountability, etc. The RBIA policy must be reviewed periodically.

2. The internal audit function shall be carried out effectively so as to ensure that it adds value to the organization. For the purpose, the ACB/Board shall approve a RBIA plan to determine the priorities of the internal audit function based on the level and direction of risk, as consistent with the entity's goals. The risk assessment of business and other functions of the organization shall at the minimum be conducted on an annual basis. Every activity / location, including the risk management and compliance functions, shall be subjected to risk assessment by the RBIA. The policy should also lay down the maximum time period beyond which even the low risk business activities / locations would not remain excluded for audit.
3. The ACB/Board is expected to review the performance of RBIA. The ACB/Board should formulate and maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The quality assurance program may include assessment of the internal audit function at least once in a year for adherence to the internal audit policy, objectives and expected outcomes. Further, ACB/Board shall promote the use of new audit tools/ new technologies for reducing the extent of manual monitoring / transaction testing / compliance monitoring, etc.

C. Senior Management

1. The senior management is responsible for ensuring adherence to the internal audit policy guidelines as approved by the Board and development of an effective internal control function that identifies, measures, monitors and reports all risks faced. It shall ensure that appropriate action is taken on the internal audit findings within given timelines and status on closure of audit reports is placed before the ACB/Board.
2. The senior management is responsible for establishing a comprehensive and independent internal audit function which should promote accountability and transparency. It shall ensure that the RBIA Function is adequately staffed with skilled personnel of right aptitude and attitude who are periodically trained to update their knowledge, skill and competencies.
3. A consolidated position of major risks faced by the organization shall be presented at least annually to the ACB/Board, based on inputs from all forms of audit.

D. Internal Audit Function

The internal audit function should assess and make appropriate recommendations to improve the governance processes on business decision making, risk management and control; promote

appropriate ethics and values within the organization; and ensure effective performance management and staff accountability, etc.

The following key-attributes need to be observed:

I. Authority, Stature, Independence and Resources

The internal audit function must have sufficient authority, stature, independence and resources thereby enabling internal auditors to carry out their assignments properly. 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.

II. Competence

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 SE.

III. Rotation of Staff

Except for the entities where the internal audit function is a specialised function and managed by career internal auditors, 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, so as to have adequate skills for the staff in the internal audit function.

IV. Tenor for appointment of Head of Internal Audit

Except for the entities 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.

V. Reporting Line

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.

VI. Remuneration

The independence and objectivity of the internal audit function could be undermined if the remuneration of internal audit staff is linked to the financial performance of the business lines for which they exercise audit responsibilities. Thus, the remuneration policies should be structured in a way to avoid creating conflict of interest and compromising audit's independence and objectivity.

VII. Responsibilities and Other General Expectations

1. The internal audit function should work on the basis of established policies and procedures as approved by the ACB/Board.
2. The internal audit 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.
3. The risk assessment in the internal audit department should be used for focusing on the material risk areas and prioritizing the audit work.
4. The risk assessment process should, inter alia, include 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.
5. 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.
6. 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 overall governance and controls in various business activities.
7. The risk assessment methodology should include, inter alia, parameters such as (a) Previous internal audit reports and compliance; (b) Proposed changes in business lines

or change in focus; (c) Significant change in management / key personnel; (d) Results of regulatory examination report; (e) Reports of external auditors; (f) Industry trends and other environmental factors; (g) Time elapsed since last audit; (h) Volume of business and complexity of activities; (i) Substantial performance variations from the budget; and (j) Business strategy of the entity vis-à-vis the risk appetite and adequacy of control.

8. For the risk assessment to be accurate, it will be necessary to have proper MIS and data integrity arrangements. The internal audit function should be kept informed of all developments such as introduction of new products, changes in reporting lines, changes in accounting practices / policies, etc. The risk assessment should invariably be undertaken on a yearly basis. The assessment should also be periodically updated to take into account changes in business environment, activities and work processes, etc.
9. Before taking up specific internal audit assignment, the plan, scope, objectives, timelines and resource allocations of the assignment should be clearly established. The scope and objectives of the assignment should be based on a preliminary assessment of the risks relevant to the business activity under review.
10. The SEs may prepare a Risk Audit Matrix based on the magnitude and frequency of risk. The Audit Plan should prioritize audit work to give greater attention to the areas of:
    a. High magnitude and high frequency
    b. High magnitude and medium frequency
    c. High magnitude and low frequency
    d. Medium magnitude and high frequency
    e. Medium magnitude and medium frequency
    f. Low magnitude and high frequency.
11. The scope of the audit and resource allocation should be sufficient to achieve the objectives of the audit assignment. The precise scope of RBIA must be determined by each SE for low, medium, high, very high and extremely high risk areas. The scope of internal audit should also include system and process audits in respect of all critical processes. The findings of such audits should also be placed before the IT Committee of the Board.
12. The internal audit report should be based on appropriate analysis and evaluation. It should bring out adequate, reliable, relevant and useful information to support the

observations and conclusions. It should cover the objectives, scope, and results of the audit assignment and make appropriate recommendations and / or action plans.

13. All the pending high and medium risk paras and persisting irregularities should be reported to the ACB/Board in order to highlight key areas in which risk mitigation has not been undertaken despite risk identification.
14. The internal audit function should have a system to monitor compliance to the observations made by internal audit. Status of compliance should be an integral part of reporting to the ACB/Board.
15. The internal audit function shall not be outsourced. However, where required, experts including former employees can be hired on a contractual basis subject to the ACB/Board being assured that such expertise does not exist within the audit function of the SE. Any conflict of interest in such matters shall be recognised and effectively addressed. Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.