Technical Guide on Risk-based Internal Audit in Banks (2024 Edition)

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Technical Guide on Risk-based Internal Audit in Banks

Board of Internal Audit and Management Accounting

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

First Edition	:	November, 2005
Second Edition	:	January, 2024
Committee / Department	:	Board of Internal Audit and Management Accounting
E-mail	:	biama@icai.in
Website	:	www.icai.org
Price	:	₹150/-
ISBN	:	81-88437-73-5
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 January | 2024 | P3539 (Revised)

Foreword

The Reserve Bank of India (RBI) mandated the Risk Based Internal Audit (RBIA) for Scheduled Commercial Banks except Regional Rural Banks in 2002. Moving further in 2021, the RBI has issued notifications requiring selected NBFCs/UCBs/HFCs to add additional best practices to be followed by the bank's internal audit team such as Authority, Stature, Independence of the Internal Audit function, Competence, Staff Rotation, Tenor for appointment for head of Internal Audit, Reporting Line, Remuneration and Outsourcing, etc.

I am happy to know that the Board of Internal Audit and Management Accounting (BIAMA) of ICAI has undertaken the project of revision of its publication "Technical Guide on Risk-Based Internal Audit in Banks" in light of aforesaid notifications and revised the same. This revised Technical Guide provides a comprehensive guidance in simple and easy to understand language on various peculiarities involved in the aforesaid notifications.

I congratulate CA. Rajendra Kumar P, Chairman and CA. Charanjot Singh Nanda, Vice-Chairman and other members of Board of Internal Audit and Management Accounting of ICAI for their sincere efforts in bringing out "Technical Guide on Risk-Based Internal Audit in Banks (2024 Edition)".

I am confident that this publication would help members to understand the Risk Based Internal Audit Framework in banks in detail and will equip them to assess risks in various operations of banks and execute the RBIA approach while conducting Internal Audits.

2nd January 2024
Delhi

CA. Aniket S. Talati
President, ICAI

Preface

The Risk-Based Internal Audit (RBIA) system was introduced in Scheduled Commercial Banks (SCBs) as part of their internal control framework in 2002. This system was further introduced for NBFCs (Non-Banking Financial Companies) and Primary (Urban) Cooperative Banks (UCBs) in 2021. This structure is primarily dependent on a clearly defined internal audit policy, functional independence with appropriate standing, efficient routes of communication, and sufficient resources for auditing with qualified professionals.

Under Risk Based Internal Audit focus shifts from present system of full-scale transaction to risk identification, prioritization of audit areas and allocation of audit resources in accordance with risk assessment of banks.

The Board of Internal Audit and Management Accounting issued "Technical Guide on Risk-based Internal Audit in Banks" in 2005. The Board is now issuing Revised Edition of this "Technical Guide" incorporating the impact of circular issued in 2021.

This publication gives a brief overview of steps to be undertaken in Risk-Based Internal Audit in Banks such as identification of auditable units, conduct risk assessment, planning Risk-Based Internal Audit. This Guide also explains factors that would be considered while conducting internal audits like functional independence, communication channels and performance evaluation.

We are immensely grateful to CA. Niranjan Joshi, CA. Giriraj Omprakash Soni and CA. Velerian Ignatius Rodrigues for sharing their experience and knowledge in review and revising Technical Guide.

We would like to thank CA. Aniket S. Talati, President, ICAI and CA. Ranjeet Kumar Agarwal, Vice President, ICAI for their continuous support and encouragement to the initiatives of the Board. We also thank the members of our Board 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, and her team for their efforts in giving final shape to the publication.

We firmly believe that this publication would help the members to not only understand the concept of risk based internal audit in banks but also learn the techniques and methodology of the same.

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. Rajendra Kumar P
Chairman
Board of Internal Audit &
Management Accounting

CA. Charanjot Singh Nanda
Vice-Chairman
Board of Internal Audit &
Management Accounting

28th December, 2023
New Delhi

Foreword to the First Edition

The banking industry has always thrown up newer opportunities and challenges, be it the statutory audits or other assignments such as concurrent audits or internal audits, etc. The dynamic environment in which this industry operates requires the members to not only use their existing skill sets to the best of their ability but also keep the same sharp enough at all times to effectively turn those challenges into opportunities. The introduction of risk-based internal audit system in banks by the Reserve Bank of India is one such opportunity in the form of a challenge for the members to contribute towards the resilience and stability of the banking industry in India.

The risk-based internal audit in banks, as against the conventional concurrent audit or internal audit in banks, is focused at improving the risk management system in banks, necessitated on account of involvement of large amount of public and government monies. Given the fact that even the implementation aspect of the risk-based internal audit system in the banking industry is in nascent and learning stages, it is necessary that our members take an initiative to properly understand the intricacies or typicalities in carrying out a risk-based internal audit and help not only the system to take firm roots in the industry but also the industry to derive maximum benefit out of the system.

I am therefore, happy to note that the Committee on Internal Audit has decided to bring out this Technical Guide on Risk-based Internal Audit in Banks for the guidance of the members. I am sure that the Committee will continue to bring out more of such topical publications for the benefit of the members.

27th October, 2005
New Delhi

Kamlesh S. Vikamsey
President

Preface to the First Edition

The banking industry in India is in a state of continuous growth and expansion, making its presence felt in all spheres of economic growth, domestic as well as global. Such marked presence at the domestic as well as international front makes it quintessential for the banking industry to benchmark with the international standards to ensure credibility, resilience as also transparency in its working in both domestic as well as international arena. Establishment of risk-based Internal Audit Systems is one such measure recommended by the Basel Committee on Banking Supervision.

The Reserve Bank of India made a beginning in this direction by issuing a circular in August 2001 requiring the banks to take necessary steps to establish a risk-based internal audit system in banks. Over the period, the regulator also brought out detailed circulars, guidance notes etc., dealing with the topic of Risk-based supervision of banks. Implementation of risk-based supervision system in banks has to the need for a system of risk-based internal audit in banks. The new system requires the chartered accountants not only to hone their existing skills but also acquire new knowledge and skills to appropriately understand the complexities of the system and make the best possible use of their knowledge and expertise to help the banking industry reap maximum benefits of the system.

In view of the above, the Committee on Internal Audit has brought out this publication, "Technical Guide on Risk-based Internal Audit in Banks" to help the members understand the fundamentals of the system. The Technical Guide is divided into four chapters. Chapter 1, Introduction, deals with aspects such as cost benefit analysis, key audit decisions such as frequency, scope, timing, size of team etc., advantages, Risk-based internal audit system vis-a-vis risk management function. Chapter 2, Steps in Risk-based Internal Audit, including risk matrix and a case study. Chapter 3 deals with other significant considerations relating to Risk-based Internal Audit in Banks and lastly, The Way Ahead. The Technical Guide also contains appendices containing the relevant circulars of the Reserve Bank of India.

I must, at this juncture, express my deep gratitude to Shri Nagesh D Pinge, Senior General Manager and his colleague Shri Srinivas Yanamandara, ICICI Bank Limited who volunteered to squeeze time out of their pressing pre-occupations to share their wealth of knowledge and experience with us and

prepared the near perfect basic draft of the Technical Guide at such short notice. The practical and clear approach of the Technical Guide definitely reflects years of hands-on experience and grasp of the authors in the area. Further, I am also thankful to my colleagues at the Committee on Internal Audit for providing valuable guidance on making the Technical Guide more useful. I also wish to express my appreciation for the support of Shri Vijay Kapur, Additional Director (Board of Studies), Smt. Puja Wadhera, Secretary, Committee on Internal Audit and Shri Nitin Singhal, Executive Officer in finalisation of the publication.

I am sure that the members would find the Technical Guide immensely useful in understanding and implementing the concept of Risk-based Internal Audit in Banks.

27th October, 2005
New Delhi

Amarjit Chopra
Chairman
Committee on Internal Audit

MEMBERS OF THE COUNCIL [2022-25]

CA. Aniket Sunil Talati, President

CA. Ranjeet Kumar Agarwal, Vice President

CA. Rajkumar Satyanarayan Adukia

CA. Piyush Sohanrajji Chhajed

CA. Chandrashekhar Vasant Chitale

CA. Vishal Doshi

CA. Durgesh Kabra

CA. Dheeraj Kumar Khandelwal

CA. Purushottamlal Hukamichand Khandelwal

CA. Mangesh Pandurang Kinare

CA. Priti Paras Savla

CA. Umesh Ramnarayan Sharma

CA. Dayaniwas Sharma

CA. Sridhar Muppala

CA. Prasanna Kumar D

CA. Rajendra Kumar P

CA. Cotha S Srinivas

CA. Sripriya K

CA. (Dr.) Debashis Mitra, Past President

CA. Sushil Kumar Goyal

CA. Rohit Ruwatia Agarwal

CA. Abhay Kumar Chhajed

CA. (Dr.) Anuj Goyal

CA. Gyan Chandra Misra

CA. Prakash Sharma

CA. (Ms.) Kemisha Soni

CA. Sanjay Kumar Agarwal

CA. Raj Chawla

CA. Hans Raj Chugh

CA. Pramod Jain

CA. Charanjot Singh Nanda

CA. Sanjeev Kumar Singhal

Shri Sanjay Kumar

Shri Ritvik Ranjanam Pandey

Shri Manoj Pandey

Shri Deepak Kapoor

Shri Rakesh Jain

Dr. P C Jain

Shri Vijay Kumar Jhalani, Advocate

Shri Chandra Wadhwa

MEMBERS OF THE BOARD OF INTERNAL AUDIT AND MANAGEMENT ACCOUNTING [2023-24]

Members from the Sitting Council

CA. Rajendra Kumar P, Chairman

CA. Charanjot Singh Nanda, Vice-Chairman

CA. Aniket Sunil Talati, President (Ex-officio)

CA. Ranjeet Kumar Agarwal, Vice-President (Ex-officio)

CA. (Dr.) Rajkumar Satyanarayan Adukia

CA. Chandrashekhar Vasant Chitale

CA. Vishal Doshi

CA. Durgesh Kumar Kabra

CA. Priti Savla

CA. Piyush S Chhajed

CA. Sridhar Muppala

CA. Prasanna Kumar D

CA. Cotha S Srinivas

CA. (Dr.) Debashis Mitra

CA. Rohit Ruwatia

CA. (Dr.) Anuj Goyal

CA. Prakash Sharma

CA. Sanjay Kumar Agarwal

CA. Pramod Jain

CA. (Dr.) Sanjeev Kumar Singhal

Shri Deepak Kapoor

Shri Chandra Wadhwa

Co-opted Members

CA. Mohit Bharti

CA. Anil Kumar Jain

CA. Sharath Kumar D

CA. Bhupal Sing Sulhyan

CA. Sarda Satish Girdharlal

CA. Pankaj Soni

CA. Nitin Hukumchand Agarwal

Special Invitees

Shri Akshay Gopal

CA. Krishnaswamy Vidyadaran

CA. P K Manoj

CA. Savio Vincent Mendonca

CA. Sana Baqai

CA. Bisworanjan Sutar

CA. Gavish Uberoi

CA. Pradeep Tyagi

CA. Tarun Kansal

Contents

Chapter 1
Introduction

Background

1.1 During the recent years, the supervisory function of the Reserve Bank of India (RBI), the banking regulator in India, is increasingly getting risk focused and the RBI has expressed its intention to move towards risk-based supervision (RBS) of banks. RBI published a discussion paper in August, 2001, 'Move Towards Risk-based Supervision of Banks', describing the scope of the RBS of banks. The discussion paper is given as Appendix I to the Technical Guide.

1.2 Under the RBS, the RBI would focus its supervisory attention on the banks in accordance with the risk profile of each bank determined by RBI. Each bank under the proposed RBS framework of RBI is expected to prepare a risk profile of its own, taking into account the various risks to which the bank is exposed. The risk profile of the bank would determine the supervisory programme comprising off-site surveillance, targeted on-site inspections, structured meetings with banks, commissioned external audits, specific supervisory directions and new policy action, as warranted. Thus, RBS requires adequate preparatory steps both at the RBI level as well as at the level of banks.

1.3 RBI has indicated the following five areas of bank level preparation for successful implementation of the RBS framework:

- Setting up of risk management architecture
- Adoption of risk focused internal Audit
- Strengthening of management information system and information technology
- Addressing Human Resources Department (HRD) issues
- Setting up of a compliance unit.

1.4 In December 2002, RBI issued a guidance note on the risk-based internal audit function in the banks, detailing the steps required to be adopted therefor. The said guidance note is given as Appendix II to the Technical Guide. Further, in February 2005, RBI issued a circular reiterating the importance of the risk-based internal audit in banks. RBI, through the said

circular, has advised the banks as to preparation of the Risk Audit Matrix based on the risk focused approach, enabling the banks to move towards the advanced approaches for determining capital charge for the operational risk under the proposed Basel II International Capital Adequacy framework. The text of the circular is given in Appendix III to this Technical Guide.

1.5 RBI vide circular no RBI/2020-21/83 Ref.No.DoS.CO.PPG./SEC. 04/11.01.005/2020-21 dated 07.01.2021 has mandated RBIA Framework for all Scheduled Commercial Banks, Local Area Banks, Small Finance Banks and Payment Banks The text of the circular is given in Appendix IV to this technical guide.

1.6 Subsequently, RBI vide circular no DoS.CO.PPG./SEC.05/11.01.005/ 2020-21dated 03.02.2021 has mandated RBIA Framework for all deposit taking NBFCs, all Non Deposit taking NBFCs with asset size of Rs.5000 Cr and above and UCBs having asset size of Rs. 500 Cr and above. The text of the circular is given in Appendix V to this technical guide.

1.7 The objective of this Technical Guide is to provide guidance to the members of the Institute, handling the statutory / internal / concurrent audit function in banking industry, as to the steps involved in the risk-based internal audit in banks.

Internal Audit - Definition, Objectives and Scope

1.8 Internal Audit is defined as follows:

Internal audit provides independent assurance on the effectiveness of internal controls and risk management processes to enhance governance and achieve organisational objectives.

1.9 Brief explanation of the key terms used above is as follows:

(i) Independence: Internal audit shall be an independent function, achieved through the position, organization structure and reporting of the internal auditor. At times, in addition to providing assurance, the internal auditor may adopt an advisory role to help an organization achieve its objectives, provided this does not compromise the independence of the internal auditor.

(ii) Internal controls and risk management are integral parts of management function and business operations. An internal auditor is expected to evaluate the design and operating effectiveness of internal controls and risk management Framework Governing Internal Audits 2 processes

(including reporting processes) as designed and implemented by the management.

(iii) Governance is a set of relationships between the company and its various stakeholders and provides the structure through which the company's objectives are achieved. It includes compliance with internal policies and procedures and laws and regulation.

(iv) Organizational objectives incorporate the interests of all stakeholders and include the short and medium term goals that an organisation seeks to accomplish.

1.10 This definition forms the underlying foundation of all the Standards on Internal Audit (SIAs) issued by the Board. Internal audit activities shall be conducted in line with the Definition of Internal Audit.

Internal Audit in Banks

1.11 The banking industry is special as it involves dealing with public money. The very nature of banking business of dealing with money requires proper checks and balances in place to ensure that the dealings are closely monitored and the risks arising out of the banking business are minimized. Towards this end, the internal audit function in a bank assists the senior management of the bank in providing an objective assurance that all the controls are well designed and effectively operated. The bank's internal audit reports are the primary source of information about the effectiveness of the risk management and internal control systems in the bank. Thus, it can be seen that internal audit has a crucial role to play in a bank's existence and growth and, therefore, needs to be effective. Towards this end, the Basel Committee on Banking Supervision of the Bank for International Settlements has also pronounced certain principles required to be followed for an effective internal audit in banks.

1.12 In India, each bank, normally, has a separate internal audit/inspection department that inspects the bank's functioning periodically and reports to the Audit Committee of the Board of Directors of the bank. Banks are expected to have sufficient resources and invest in training their staff to conduct internal inspections. 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 Senior Executives. Any conflict of interest in such matters shall be recognized and effectively addressed.

Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.

Additionally, banks have also either instituted in-house departments for carrying out "systems audits" or have outsourced this specialized field. Systems Audit focuses on whether the internal procedures and controls are being adhered to at the operational level and whether the existing systems are adequate and commensurate with the requirement of the changing business environment.

1.13 The effectiveness of internal audit function of banks is assessed during the course of on-site inspection by RBI. Supervisory concerns thrown up by internal audit/inspection provide pointers or indicators for on-site inspection of RBI.

Risk-based Internal Audit

1.14 A sound internal audit function plays an important role in contributing to the effectiveness of the internal control system. Until recently, the internal audit system in banks had been concentrating on transaction testing, testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, and adherence to legal and regulatory requirements. However, in the changing scenario, such testing by itself is not sufficient for the purpose of providing an objective assurance on the functioning of internal controls by the internal audit function.

1.15 During recent times, in addition to the traditional risks that the banks are exposed to, the increasing global scale operations of banks, impact of the information technology on the banking systems and processes, have exposed the business of the banks to newer risks. The management of these risks is crucial for the success of any banking organisation. This requires the independent functions such as compliance and internal audit to be more risk focused to ensure that the risks are being identified, assessed and managed effectively on a bank-wide basis. Towards this end, RBI felt that there is a need for widening as well as redirecting the scope of internal audit to evaluate the adequacy and effectiveness of risk management procedures and internal control systems in the banks.

Key Elements of the RBIA as Recommended by RBI

1 The internal audit shall undertake an independent risk assessment **for focusing on the material risk areas and prioritizing the audit work**.

2 The risk assessment process should, inter-alia, include identification of inherent business risks and making a risk-matrix for both the factors viz., inherent business risks and control risks.

3 The basis for determining the level (high, medium, low) and trend (increasing, stable, decreasing) of inherent business risks and control risks should be mentioned.

4 Both quantitative and qualitative approaches may be used for risk assessment. 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.

5 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;

(j) Business strategy of the entity vis-à-vis the risk appetite and adequacy of control.

6 For the risk assessment to be accurate, it will be necessary to have proper MIS and data integrity arrangements.

7 The SEs may prepare a Risk Audit Matrix based on the magnitude and frequency of risk.

8 The scope of the audit and resource allocation should be sufficient to achieve the objectives of the audit assignment.

9 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.

10 The internal audit function should have a system to monitor compliance with the observations made by internal audit. Status of compliance should be an integral part of reporting to the ACB/Board.

11 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 recognized and effectively addressed. Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.

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, and evaluation of the risk management system and control procedures in various areas of operations. This will also help in anticipating areas of potential risk and mitigating such risk.

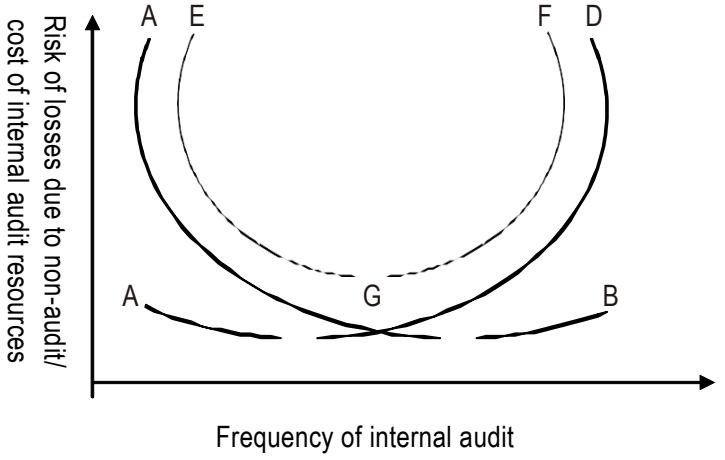
Cost-benefit Analysis

1.16 The argument for the risk-based internal audit can be further supplemented by the cost-benefit analysis of the internal audit function. In this connection, it should be noted that internal audit is invariably a cost center in any organisation. It is, therefore, necessary that the internal audit function develops and implements an effective, long range internal audit plan so that the benefits derived therefrom effectively exceed the costs allocated to the function.

1.17 The primary objective of internal audit is to provide an objective assurance on the functioning of internal controls in the bank. However, there is an inherent risk that the internal audit function may not reveal all the weaknesses in the internal controls. This may lead to risk of losses in terms of fraud, including embezzlement, and misappropriation of assets. To minimize these risks, one suggestive approach is to make the internal audit function more continuous, i.e., audit the different departments more frequently. For example, increase in frequency of internal audit may result in reduction in expected losses but increases the cost of audit function. On the other hand, decrease in frequency of internal audit, though may reduce the costs of audit

function, results in risk of frauds and errors leading to financial and other losses to the bank. Thus, the decision to increase the frequency of internal audit should be based on a careful analysis of the trade-off between the cost associated with carrying out frequent internal audits *vis a vis* the expected losses arising out of not carrying out internal audit. This trade-off can be best achieved with the risk-based internal audit, which aims at optimal utilization of internal audit resources with an enterprise-wide risk management perspective.

This can be pictorially depicted as follows:



1.18 In the above diagram, the curve AB denotes the risk curve, which represents that as the frequency of internal audit increases, the risk of non-detection of ineffective internal controls (and consequently the expected losses) decreases. The curve CD denotes the cost curve, which represents that as the frequency of internal audit increases, the costs associated with carrying out internal audit increase. The curve EF denotes the total cost curve (which includes the cost of non-detection of ineffective internal controls in terms of expected losses and the cost of resources allocated to internal audit function), which decreases upto a certain level and thereafter increases. Point G is where the total cost is at its minimum and is ideal for a risk-based scenario.

Key Audit Decisions of a Risk-based Internal Audit

1.19 Keeping the above theoretical background in mind, it is important to note that the risk-based internal audit is an important tool in aiding the management decision in relation to the following aspects of internal audit function.

Frequency of Audit

1.20 The risk-based approach of internal audit assists the management in deciding the frequency of the audit. After undertaking the risk assessment of the auditee units in the audit universe, these units can be categorized on the basis of the risk parameters as high, medium or low risk units. These units can then be subjected to the internal audit at a frequency suited to their risk profile. This can be achieved by subjecting the units with a high-risk profile to internal audit more frequently than the units that exhibit a low-risk profile. Thus, risk assessments of audit units determine the frequency of the internal audit and thus assist in optimal allocation of audit resources.

Scope of Audit

1.21 Scope of internal audit refers to the extent to which the testing of internal controls in an internal audit assignment should be undertaken. As a general principle, high-risk audit units such as treasury division of the bank should be subject to 100% transactions testing. However, units with a relatively low-risk profile activity such as allocation of the lockers to the customers may be subject to a sample testing. In this connection, members are also advised to refer to the Auditing and Assurance Standard (AAS) 15, Audit Sampling, for guidance on using statistical sampling techniques for undertaking audit assignments. However, the sampling technique proposed to be so adopted should first be placed for the approval of the audit committee, if any.

Timing of Internal Audit

1.22 It is a known fact that no internal audit function has the resources to audit all the auditable units simultaneously. Therefore, the third key decision that can be taken using the risk-based internal audit is to ensure that the riskier unit is subject to audit sooner than the less risky audit units. This can be achieved by adoption of a *fixed timing policy* of internal audit whereby the less risky units are subject to internal audit at known fixed intervals. However, the high-risk audit units can be subject to a *random timing policy* (where the

frequency and timing of audits is unpredictable to the auditable unit). Surprise visits and snap audits, in addition to full-scale internal audit, are components of random timing policy. For auditable units with medium-risk profile, internal audit should be based on conditional timing policy, under which internal audits are scheduled when units exhibit a deterioration of controls or performance along with some key dimension. The deterioration can be observed on the basis of analysis and scrutiny of the key returns on the performance of the auditable unit.

Size of the Internal Audit Team

1.23 Risk-based internal audit approach assists the management (where the internal audit function is in-house) and the audit firm (where the internal audit function is outsourced) in determination of the size of the internal audit team. If risk factors reflect the management concerns, then they can be used as a basis for establishing the size of the internal audit team appropriate to address the most important audit units.

1.24 To ensure that the cost factors are effectively factored into audit decision and the key audit decisions, as explained above, are more risk-based, banks and certain NBFCs are advised by the RBI to implement the RBIA Framework by 31.03.2022 vide circular dated 03.02.2021 which includes, in addition to selective transaction testing, an evaluation of the risk management systems and control procedures prevailing in various areas of a bank's operations. The implementation of risk-based internal audit would mean that greater emphasis is placed on the internal auditor's role in mitigating risks. While focusing on effective risk management and controls, in addition to appropriate transaction testing, the risk-based internal audit would not only offer suggestions for mitigating current risks but also anticipate areas of potential risks and play an important role in protecting the bank from various risks.

Advantages of Risk-based Internal Audit

1.25 The advantages of risk-based approach of the internal audit function are as follows:

- It appropriately defines the audit universe and identifies the auditable units within the entity for which these analyses would be carried out.
- It assists the management in identification of appropriate risk factors to reflect the management's concerns.

- It results in development of an appropriate format for evaluating risk factors so that the more important risk factors play a more prominent role in the risk assessment process than less important risk factors.
- It develops a combination rule for each audit unit, which will properly reflect its riskiness
- over several risk factors that have been identified and a method of setting up audit priorities for the audit units.
- It results in appropriate audit coverage plan, which provides a roadmap for the management of internal audit staff skills so that they are available to carry out audits of appropriate scope when they are needed the most.
- This risk-based internal audit results in a process oriented audit with a risk management perspective, which gives advice to management on the steps to be taken for effective risk management on a bank-wide basis.

Risk-based Internal Audit vs. Risk Management Function

1.26 Though both the risk management and the internal audit (risk-based) functions deal with the risk management systems of the bank, it is necessary to distinguish both the functions. The risk management function of a bank focuses on areas such as identification, monitoring and measurement of risks, development of policies and procedures, use of risk management models, etc. Thus, the end result of the risk management function is development of appropriate policies and procedures for effective risk management on a bank-wide basis.

1.27 The concept of risk identification and the assessment is also undertaken under the risk-based internal audit framework of the banks. However, unlike risk management function, the risk- based internal audit, undertakes 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 those inherent business risks.

1.28 The primary difference between the two functions *viz.*, risk management and the internal audit, therefore, is the purpose for which the tool of the risk assessment is used. Under the former function, it is used for development of risk management policies and procedures whereas in the later function, the

same is used for formulation of appropriate risk-based audit plan resulting in optimal usage of internal audit resources on a risk sensitive basis.

1.29 Being an independent and key function in the bank, the risk management department should also be subjected to risk assessment by the risk-based internal audit process and should be audited in accordance with the risk-based audit plan duly approved by the Audit Committee of the Board.

Chapter 2
Steps in Risk-based Internal/ Concurrent Audit in Banks

Introduction

2.1 The adoption of the risk-based approach to the internal audit requires the following four major steps to be adopted by the internal auditors:

Step 1: Preparation

2.1.1 The internal auditor should treat the risk-based internal audit assignment as a separate project since it requires significant audit resources and time. For this purpose, it is absolutely essential that the preparation for the project is meticulously planned such that the risk assessment exercises are properly undertaken at a later stage. The output under this step would not only define the size and structure of the internal audit function in the bank, where the bank has an in-house internal audit function or the size of the internal audit team where the internal audit function is outsourced, but also serves as a basis for assignment of clear roles and responsibilities to the participants in the internal audit exercise and communication of the same to them.

Step 2: Identification of auditable units

2.1.2 Identification of auditable units constitutes the second step in the risk-based internal audit. Identification of auditable units is relevant to understand the entire audit universe covered under the scope of the risk-based internal audit. It, thus, leads to the conclusion of the uncovered auditable units and the resultant residual risk of non-audit of those auditable units.

2.1.3 Further, the proposed new capital adequacy framework of RBI (based on the Basel Committee's International Capital Adequacy Framework) also requires identification of business units as a first step in determination of the capital charge required for the operational risk. It would be a prudent decision to combine both the capital adequacy assignment (from an operational risk management perspective) with the risk-based internal audit assignment, as both are complementary to each other.

Step 3: Conduct risk assessment

2.1.4 The next step is to identify the risks and categorize the risks as high, medium and low, depending upon the nature of the risks. Risks in the context of the internal audit of banks can be classified as inherent banking business risks such as credit and market risks. In recent years, given the significant volumes of transactions in the retail portfolio of the bank, a new risk, styled as "operational risk", has emerged gradually. These risks can be mitigated by adoption of risk management and internal control policies and procedures, formulated by the Board of Directors. However, adoption of appropriate policies and procedures still carries a risk called as control risk that is the risk of failure of control policies and procedures in detection of a material risky situation and addressing it appropriately. In addition to identification of the quantum of the risks at this stage, the trend of the risks (increasing, stable, decreasing) is also identified at this stage.

2.1.5 Once the risks are classified under inherent business risks and the control risks, each of the auditable units is to be assessed with reference to the identified risk parameters. For this purpose, it is necessary to categorize the entire banking business as identifiable auditable units, each prone to a different level of a risk.

2.1.6 The objective of the risk assessment process is to draw up a risk-matrix, taking into account both the factors *viz*., inherent business risks and control risks identified in the earlier step. This risk matrix appropriately places all the auditable units into one among the three categories of risk profiles-high, medium or low.

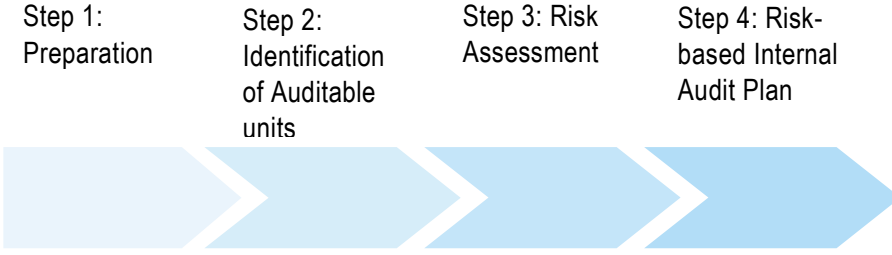
2.1.7 The internal audit function, whether in-house or outsourced, should have in place, an independent risk assessment system for focusing on the material risk areas and prioritizing the audit work. The methodology may range from a simple analysis of why certain areas should be audited more frequently 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.

Step 4: Risk-based internal audit plan

2.1.8 Once the risk matrix is prepared, a risk-based audit plan based on the risk profile of the audit units is prepared. This involves decision to be taken on the frequency, timing and the scope of the internal audit of the auditable unit. These decisions are based on the internal audit priorities and keeping in view

the objective of internal audit function as a risk management tool. The risk-based internal audit plan as prepared by the internal audit function of the bank is duly approved by the Audit Committee of the Board of Directors of the Bank.

2.1.9 The above process is diagrammatically represented as fellows



Step 1:	Step 2:	Step 3:	Step 4:
• Establish the Project • Specify Obectives • Creation of Organisation Structure	• Identify the auditable units • Determine the risk of non-audit of unidentifiable auditable units • Categorize the risks	• Identify the auditable units • Conduct risk assessment of auditable unit • Categorize the auditable unit	• Finalization of the risk-based internal audit plan • Submission and approval from the Audit Committee

2.1.10 Each of the above steps are described as follows:

Preparation

2.1.11 The first step involves the initiation of the risk-based internal audit process at the bank. The idea at this stage is to treat the risk-based audit concept as a distinct project with an objective of formulation of audit plan with more risk focus at the end of the project. For this purpose, it is absolutely necessary at this stage to:

- Establish the project team
- Clarify the roles and responsibilities of the project team
- Scheduling the project tasks
- Communication

2.1.12 Depending upon the size of the bank, the risk-based internal audit project can be handled by a committee of senior executives (SE) with the responsibility of formulating a suitable action plan. As a internal / concurrent auditor a small team of audit professionals can be engaged in conducting the RBIA. While choosing the members for this assignment, it should be ensured that they have adequate internal audit and risk management expertise. Few criteria for selection of professionals for this assignment include, experience in conducting risk assessments, audit planning experience and ability to analyze and synthesize a wide range of information.

2.1.13 After choosing appropriate professionals for the assignment, it is important to clarify the roles and responsibilities of the team members of the risk-based internal audit assignment. This involves designation of a senior professional as the project authority, having overall responsibility for the entire project. The team leader would be assisted by the team members who would be responsible for proposing and executing an approach for implementation of the project. The team would have extensive interactions with the senior management of the auditable units who would be responsible for participation in meetings for identification and assessing the key risks faced by the auditable units.

2.1.14 As the project gets started, it is important to ensure that the project is accomplished with tight deadlines and reporting responsibilities. This requires formulation of a project plan and providing the team members with appropriate tools such as policies/procedures, checklists for evaluation and the software, if any, necessary to execute the plan and document the results. Effective planning demands communication of the established approach to all the participant units such that all the members of the team are at the same wavelength.

Identification of auditable units

2.1.15 The next step towards risk-based internal audit is to identify all the activities that are susceptible to the inherent risk. In line with the proposed Operational Risk Management framework enunciated by RBI, the identification of auditable units can be taken at three different levels as follows:

Level 1 - lists the main business groups such as corporate finance, trading and sales (treasury function), retail banking, commercial banking, etc.

Level 2 - lists the product teams in these business groups such as transaction banking, trade finance, general banking, cash management services, etc.

Level 3 - lists out the products offered in these business groups such as import bills, letter of credit, bank guarantee under trade finance, etc.

2.1.16 Identification of the auditable units at the first level itself is required for the purpose of the risk- based audit plan. However, the sub-classification into further levels helps the internal audit team to identify and assess the applicable risks to the auditable unit in a more systematic manner.

Conduct risk assessment

2.1.17 It should be noted that there are two types of risks in banking business in the context of risk- based internal audit. One that is inherent in the business operations of the bank itself, such as the credit, market and operational risk and the other one is the risk that the controls designed to mitigate these risks may not be effective, typically termed as control risk. Thus, inherent business risks indicate the intrinsic risk in a particular area/activity of the bank. Control risks arise out of inadequate control systems, deficiencies/gaps and/or likely failures in the existing control processes.

2.1.18 Hence, while undertaking a risk identification exercise under the risk-based audit programme, one should keep in mind that the risk assessment of an auditable unit is largely based on both the inherent and the control risks and should be judged in combination thereof.

Key Factors Relevant for Risk Assessment

2.2 Before understanding the risk assessment exercise as per the steps enumerated subsequently, it should be borne in mind that the risk assessment is largely determined by factors such as:

- Previous internal audit reports and compliance
- Proposed changes in business lines or change in focus
- Significant change in management/key personnel
- Results of latest regulatory examination report
- Reports of external auditors
- Industry trends and other environmental factors
- Time lapsed since last audit
- Volume of business and complexity of activities
- Substantial performance variations from the budget

Keeping the above factors in mind, the risk assessment exercise can be undertaken using the following steps.

Inherent Business Risks

2.3 Banks are subject to wide variety of risks in the areas of their operation. All of them can be broadly categorized as credit, market and operational risks. Each of these risks are explained as follows:

Credit Risk[1]

2.3.1 Credit risk is defined as the possibility of losses associated with diminution in the credit quality of borrowers or counterparties. In a bank's portfolio, losses stem from outright default due to inability or unwillingness of a customer or counter party to meet commitments in relation to lending, trading, settlement and other financial transactions. Alternatively, losses result from reduction in portfolio value arising from actual or perceived deterioration in credit quality. Credit risk emanates from a bank's dealings with an individual, corporate, bank, financial institution or a sovereign. Credit risk may take one or more of the following forms:

- *Direct lending:* principal and/or interest amount may not be repaid
- *Guarantees or letters of credit:* funds may not be forthcoming from the constituents upon crystallization of the liability
- *Cross-border exposure:* the availability and free transfer of foreign currency funds may either cease or the sovereign may impose restrictions

2.3.2 Credit risk is more relevant to the auditable units where credit lending function is exercised such as the corporate/retail lending function of the banks. The extent of credit risk may also substantially differ from the units which are dedicated to credit sanctions such as the Credit Department where the risk is higher whereas in other functions where credit sanction is incidental to the main function (such as in branches of banks where sanction of loan against deposits is only incidental as per the delegation of financial powers to the branch manager), the credit risk impact might be lower.

[1] Please refer Reserve Bank of India Guidance Note on Credit Risk Management October 12, 2002

Market Risk[2]

2.3.3 Market Risk may be defined as the possibility of loss to a bank caused by changes in the market variables. Market Risk is the risk to the bank's earnings and capital due to changes in the market level of interest rates or prices of securities, foreign exchange and equities, as well as the volatilities of those changes. Besides, it is equally concerned about the bank's ability to meet its obligations as and when they fall due. Market risk manifests itself into various forms such as:

- *Liquidity risk:* Liquidity risk is the potential inability of the bank to meet its liabilities as and when they become due. It arises when the banks are unable to generate cash to cope with a decline in deposits or increase in assets. It originates from the mismatches in the maturity pattern of assets and liabilities.
- *Interest rate risk:* It is the risk where changes in market interest rates might adversely affect a bank's financial condition.
- *Foreign Exchange Risk:* It may be defined as the risk that a bank may suffer losses as a result of adverse exchange rate movements during a period in which it has an open position, either spot or forward, or a combination of the two, in an individual foreign currency.
- *Treasury operations:* the payment or series of payments due from the counter parties under the respective contracts may not be forthcoming or ceases
- *Securities trading businesses:* funds/ securities settlement may not be effected

Operational Risk

2.3.4 Operational risk has been defined by the Basel Committee on Banking Supervision as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risk may manifest itself in a variety of ways in banking industry such as internal/external fraud, client/product/business practices, damage to physical assets, business disruption and system failure etc. Examples of various contributing factors for operational risks are as follows:

[2] Please refer Reserve Bank of India Guidance Note on Market Risk Management October 12, 2002

- *People risk:* This depends upon the placement, competency of the employees of the bank and the work environment, motivation and turnover/rotation in a bank.
- *Process risk:* Risk arising out of execution of transactions involving violation of controls, operational disruptions, exceeding of limits, money laundering, non-observance of contractual commitments, etc.
- *Systems risk:* This is the combination of both technology risks resulting in system failure, programming error, communication failure, etc., coupled with the MIS risk.
- *Legal and regulatory risk:* Risk of failing to comply with laws and regulations.
- *Reputational risk:* The risk of loss of the reputation of the bank in the general public due to the failure to conduct its business up to the standards expected.
- *Event risk:* Risk of unanticipated changes in external environment other than macro economic factors.

Control Risk

2.4.1 Once the risks are identified as above, it should be ensured that the bank has appropriate risk management systems in place, which define the control environment and prescribe the control procedures for mitigation of the above risks. In this context, it is relevant to understand the concept of the control environment and the control procedures as risk management tools.

Control Environment

2.4.2 The Auditing and Assurance Standard 6, Risk Assessments and Internal Control defines the term 'control environment' as “the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance in the entity”. The control environment has an effect on the effectiveness of the specific control procedures and provides the background against which other controls are operated. A strong control environment, for example, one with tight budgetary controls and an effective internal audit function, can significantly complement specific control procedures.

2.4.3 In a banking organisation, the factors reflected in the control environment include:

- Organizational structure of the bank and the methods of assigning authority and responsibility including segregation of duties and supervisory functions
- Role of Board of Directors and its committees in defining control environment and adopting appropriate control procedures
- Management's philosophy and operating style
- Management's control system including the internal audit function, personnel policies and procedures

Control Procedures

2.4.4 The Auditing and Assurance Standard 6, Risk Assessments and Internal Control defines the term 'control procedures' as “those policies and procedures, in addition to the control environment, which the management has established to achieve the entity's specific objectives”. In the context of banking organisation, the specific control procedures include:

- Approving and controlling of documents
- Segregation of duties and supervisory functions
- Decision making subject to the 'four eyes/six eyes ' (those of the maker, checker, Reviewer) concept of management
- Reporting and reviewing of exceptions
- Comparing the internal data with external sources of information
- Restricting direct access to assets, records and information
- Information system controls, which include controls over changes to computer programs and access to data files
- Two factor authentication in addition to password

2.4.5 As observed above, while the establishment of the control environment is the responsibility of the top management of the bank, designing of appropriate control procedures for mitigation of risks is the responsibility of the risk management department. An independent risk management function, operating in a proactive control environment, designs the control procedures, which are to be implemented on a bank-wide basis.

Internal audit and control risk

2.4.6 The internal auditor, while developing a risk-based internal audit plan should obtain an understanding of the control environment sufficient to assess management's attitudes, awareness and actions regarding internal controls and their importance in the bank. The internal auditor should also obtain an understanding of the control procedures sufficient to develop the risk-based audit plan.

2.4.7 From the point of view of risks, the role of internal audit at this juncture is twofold:

- Ascertaining the inherent risk of the risk management function and identifying the extent of the areas where the control procedures are not established by the risk management function
- Evaluating the risk involved in the control procedures designed for mitigation of risks

Preliminary assessment of control risk

2.4.8 After obtaining an understanding of the control environment and control procedures and having satisfied himself that control procedures are existent in all the auditable units, the internal auditor should make a preliminary assessment of control risk. The preliminary assessment of control risk is the process of evaluating the likely effectiveness of an entity's control environment and the control procedures in managing the inherent business risks. The preliminary assessment of control risk is based on the assumption that the controls operate generally as designed and described and that they operate effectively throughout the period of intended reliance. There will always be some control risk because of the inherent limitations of any internal control system.

2.4.9 The preliminary assessment of control risk should be high unless the auditor is able to identify control procedures relevant to the inherent business risk of an auditable unit and ensuring that control procedures are adequate to mitigate the business risk. When control risk is assessed at less than high, the internal auditor would also document the basis for the conclusions.

2.4.10 At this stage the internal auditor should document the understanding obtained of the bank's control environment and the control procedures. He should also decide whether the situation warrants an independent test of control procedures to be performed for understanding the control risk involved.

2.4.11 Different techniques may be used to document information relating to control environment and procedures. Selection of a particular technique is a matter of the internal auditor's judgment. Common techniques, used alone or in combination, are narrative descriptions, questionnaires, checklists and flow charts. The size and complexity of the auditable unit and the nature of the inherent business risks to which the auditable unit is exposed, influence the form and extent of this documentation. Generally, the more complex the control environment and procedures and the more extensive the internal auditor's procedures, the more extensive the auditor's documentation will need to be.

Tests of control

2.4.12 Wherever necessary, based on the preliminary assessment of control risk, the internal auditor can undertake the tests of control as a one-time exercise to understand the operation of internal controls designed for an auditable unit in a systematic manner. Tests of control may include:

- Inspection of documents supporting transactions and other events to gain audit evidence that internal controls have operated properly, for example, verifying that a transaction has been properly authorised
- Inquiries about, and observation of, internal controls, which leave no audit trail, for example, determining who actually performs each function and not merely who is supposed to perform it
- Re-performance of internal controls, for example, reconciliation of bank accounts, to ensure they were correctly performed by the entity
- Testing of internal control operating on specific computerized applications or over the overall information technology function, for example, access or program change controls

2.4.13 The internal auditor should obtain audit evidence through tests of control to support any assessment of control risk, which is less than high. The lower the assessment of control risk, the more evidence the internal auditor should obtain that internal control systems are suitably designed and operating effectively.

2.4.14 When obtaining audit evidence about the effective operation of internal controls, the auditor considers how they were applied, the consistency with which they were applied during the period and by whom they were applied. The concept of effective operation recognizes that some deviations may have occurred. Deviations from prescribed controls may be caused by such factors

as changes in key personnel, significant seasonal fluctuations in volume of transactions and human error. When deviations are detected, the internal auditor makes specific inquiries regarding these matters, particularly, the timing of staff changes in key internal control functions. The auditor then ensures that the tests of control appropriately cover such a period of change or fluctuation.

2.4.15 Based on the results of the tests of control, the auditor should evaluate whether the internal controls are designed and operating as contemplated in the preliminary assessment of control risk. The evaluation of deviations may result in the internal auditor concluding that the assessed level of control risk needs to be revised. In such cases, the internal auditor would modify the nature, timing and extent of planned substantive procedures.

Qualitative and quantitative approaches for risk assessment

2.4.16 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 through the use of both qualitative and quantitative 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. In order to focus attention on areas of greater risk to the bank, an activity wise and location-wise identification of risk should be undertaken.

2.4.17 In this connection, the principle enunciated in the Auditing and Assurance Standard (AAS) 20, Knowledge of the Business, should be noted which is as follows:

"In performing an audit of financial statements, the auditor should have or obtain knowledge of the business sufficient to enable the auditor to identify and understand the events, transactions and practices that, in the auditor's judgment, may have a significant effect on the financial statements or on the examination or audit report. Such knowledge is used by the auditor in assessing inherent and control risks and in determining the nature, timing and extent of audit procedures."

Risk Matrix

2.4.18 After the inherent and control risks are identified, the auditor should map both the risks to ensure that the combination of both the risks are at an

acceptable level. For this purpose, the auditor has to juxtapose the inherent business risks and the control risk in a systematic manner. The resultant scenario determines the risk appetite of a particular audit unit, which is the key input for determination of risk-based audit plan for that particular auditable unit. A typical risk matrix looks as follows:

Risk Matrix				
Inherent risk	High	A	B	C
	Medium	D	E	F
	Low	G	H	I
		Low	***Medium***	***High***
	Control risk			

An explanation of the underlying the risk appetite of the above auditable units is as follows:

S. No	Auditable Unit	Nature of risk	Explanation
1.	A	High Risk	Although the control risk is low, this is a High Risk area due to high inherent business risks.
2.	B	Very High Risk	The high inherent business risk coupled with medium control risk makes this a Very High Risk area
3.	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.
4.	D	Medium Risk	Although the control risk is low this is a Medium Risk area due to medium inherent business risks.

5.	E	High Risk	Although the inherent business risk is medium this is a High Risk area because of control risk also being medium.
6.	F	Very High Risk	Although the inherent business risk is medium, this is a Very High Risk area due to high control risk.
7.	G	Low Risk	Both the inherent business risk and control risk are low.
8.	H	Medium Risk	The inherent business risk is low and the control risk is medium.
9.	I	High Risk	Although the inherent business risk is low, due to high control risk this becomes a High Risk area.

Risk-based Internal Audit Plan

2.5.1 Once the risk assessment exercise is undertaken by the internal auditor and the auditable units are arranged as per the risk matrix as explained above, the next step is to devise the risk-based audit plan detailing out the priorities, nature, timing and extent of internal audit procedures in an auditable unit with reference to the risk categorization of the auditable unit. Internal audit priorities are driven primarily by the need to assess the risk management practices and controls to varying levels of assurance or by a need for advice.

Scope

2.5.2 The precise scope of risk-based internal audit must be determined by each bank for low, medium, high, very high and extremely high risk areas. However, as per the extant guidelines of RBI, at the minimum, it must review/report on:

- Process by which risks are identified and managed in various areas
- The control environment in various areas
- Gaps, if any, in control mechanism which might lead to frauds, identification of fraud prone areas
- Data integrity, reliability and integrity of MIS

- Internal, regulatory and statutory compliance
- Budgetary control and performance reviews
- Transaction testing/verification of assets to the extent considered necessary
- Monitoring compliance with the risk-based internal audit report
- Variation, if any, in the assessment of risks under the audit plan vis-à-vis the risk-based internal audit.

2.5.3 The scope of risk-based internal audit 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.

Contents of Risk-based Audit Plan

2.5.4 The contents of risk-based audit plan are normally as follows:

(i) Audit Universe: The risk-based audit plan at the outset lists down the entire auditable units, which are subject to the internal audit in one form or other. An explanation of the nature and scope of the auditable units is provided under this section.

(ii) Priority: Each auditable unit is to be assigned a risk category based on the risk assessment of the auditable unit as outlined above. For this purpose, it is important that the plan should give importance to the magnitude and the frequency of the risks also as observed in the risk assessment exercise for the purpose of conducting of internal audit in respect of the respective auditable unit. The audit plan should prioritize audit work to give greater attention to areas of:

- High Magnitude and high frequency
- High Magnitude and medium frequency
- Medium magnitude and high frequency
- High magnitude and low frequency
- Medium Magnitude and medium frequency.

(iii) Type of the internal audit assignment: The shape and the form of the internal audit assignment should be clearly defined. Two types of the internal audit assignment are particularly relevant in this connection:

- Assurance: This type of internal audit assignment is designed to provide senior management with assurance services. Assurance services are objective examinations of evidences for the purposes of providing an independent assessment of risk management.
- strategies and practices, management control frameworks and practices and information used for decision making and reporting.
- Consulting: Consulting assignments are designed to provide senior management with assistance. These assignments are not designed to provide assurance as mentioned above.

(iv) Frequency: The risk-based internal audit plan should also outline the frequency within which the auditable units are subject to the internal audit. It should be noted that the frequency of the audit is a function of the internal audit priorities as outlined above and the available internal audit resources etc. However, all the auditable units should be subject to one form or other of internal audit at intervals as decided by the management but preferably, at least once in three years.

(v) Extent of testing: The primary focus of risk-based internal audit will be to provide reasonable assurance to the Board and top management about the adequacy and effectiveness of the risk management and control framework in the banks' operations. While examining the effectiveness of the control framework, the risk-based internal audit should report on proper recording and reporting of major exceptions and excesses. As per the extant guidelines of RBI, transaction testing would continue to remain an essential aspect of risk-based internal audit of banks. The extent of transaction testing would be determined on the basis of risk assessment. Illustratively, the bank should undertake 100 per cent transaction testing if an area falls in cell “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 banks may also consider transaction testing with an element of surprise in respect of low risk areas, which would be audited at relatively longer intervals.

(vi) Resource requirements: The plan for risk-focused audit should also specify an estimated range of level of effort required to carry out the project. The effort estimate should take into consideration the following factors:

- Nature of internal audit assignment (consulting, assurance)
- The scope of the internal audit assignment (including considerations of

audit period, business process and the business objectives to be assessed)

- The complexity of auditable unit, business processes and systems in scope
- The availability of internal audit and subject matter expertise
- The quality and quantity of existing documentation in the subject area
- The audit approach and techniques to be used (e.g., interviews, transaction sampling, workshops, computer assisted audit tools, etc.).

As per the guidelines of RBI, the internal audit function should be provided with appropriate resources and staff to achieve its objectives under the risk-based internal audit system. The staff possessing the requisite skills should be assigned the job of undertaking risk-based internal audit. They should also be trained periodically to enable them to understand the bank's business activities, operating procedures, risk management and control systems, MIS, etc.

(vii) Submission of the internal audit plan: The results of the above process including toolset requirements for the risk-based internal audit should be presented and validated by the senior management. It is important to engage senior management in this process to seek their final input on the highest priorities for internal audit and to ensure that there is adequate support for the rationale provided. It is, therefore, recommended to seek the views of the senior management of the auditable units on the risk-based internal audit plan and incorporate the necessary suggestions in the audit plan. The final plan as acceptable to the internal audit function and the auditable units is to be placed before the Audit Committee of the Board of Directors for their final approval.

CASE STUDY

Risk Assessment of an Auditable Unit-Retail Loan Department

Let us consider, for example, one of the identified auditable units by the internal auditor as “Retail Loan department”. This includes further sub-units such as home loans, commercial vehicle loans, personal loans, auto loans and two wheeler loans departments. Once the auditable unit is identified, the following steps are to be undertaken for ensuring the risk appetite of the retail loan department.

Identification of inherent business risks: In retail loan portfolio, the major inherent business risk is the credit risk, i.e., risk of default by a retail borrower.

Identification of control procedures: To ensure that the credit risk is appropriately taken care of, adequate control policies and procedures are to be formulated by the retail risk management department of the bank. These procedures might include:

- Devising the scorecard approaches specifying the criteria for acceptance of customer.
- Segregation of the functions of sourcing the borrowers and sanctioning of the loans.
- Establishment of an independent risk control unit, which undertakes the verification of the accuracy of the loan documents along with the necessary supplements documents submitted by the borrower including their authenticity itself.
- Designing a proper MIS framework resulting in appropriate monitoring of the portfolio including periodic, exception reports being generated.
- Ensuring adequate personnel to undertake the study of the movement of the retail loan portfolio with particular emphasis on the trend of the delinquency ratios being observed over a period of time.
- Creation of a separate loan collection network for following up with the delinquent borrowers.

The formulation of the above control procedures is, as mentioned above, the responsibility of the risk management department. However, once the procedures are formulated there is a risk that they may not be properly implemented due to failure of people, process or systems. This risk is technically termed as operational risk.

Preliminary assessment of the control risk

The internal auditor who is undertaking the risk assessment of the retail loan department of a bank has to primarily understand the procedures determined for mitigating the credit risk inherent in the retail loan portfolio. While understanding the procedures, he may come across certain areas in the retail loan portfolio, which may not be covered by the above procedures. For example, the sourcing of the borrowers function has been entrusted to an external agency by the bank. In that situation, the outsourcing risks arising out of the external agency arrangement may be of particular concern for

determining the operational risk of the retail loan department. These outsourcing risks include, risk of fake field investigation, dubious reports being submitted by the external agency, etc. The internal auditor in such case can suggest to the risk management department, the risk mitigants to be formulated to obviate the outsourcing risks. However, it should be noted that the ultimate responsibility of designing appropriate control procedures lies with the risk management department.

While undertaking the preliminary assessment of the control risk, the internal auditor should determine the likelihood of the risk of a particular process or function not adequately covered by the control procedures. He should also, in such circumstances, understand the quantum of the risk being identified and document the internal audit procedures undertaken to reach such conclusion.

Risk Rating

For the purpose of risk assessment, the internal auditor may adopt a rating criteria for assessing the risks, both inherent and control, which would assist him in objective evaluation of the risks in the auditable unit. This exercise requires the internal auditor to rate the risk posed by the auditable unit on a pre- defined rating scale where the low rating would indicate a low risk and *vice versa.* Such an exercise would result in the standardization of the risk assessment and assist the internal auditor in documenting the steps undertaken for the risk assessment.

Tests of controls

After the preliminary assessment, the internal auditor, if he feels that the situation demands that the tests of controls should be undertaken, should take appropriate steps to independently test the operation of the internal control procedures. For this purpose, he may take up appropriate credit files and try to evidence the observance of the prescribed procedures. These tests of controls further supplement the preliminary assessment of internal control in reaching a conclusion about the control risk of the retail loan department.

Risk Mapping

After identification of the inherent and the control risks of the retail loan department, the internal auditor is required to make a judgment about the nature of these risks as high, medium or low depending on the results of the audit procedures as above, including the results of the tests of the control undertaken, if any, and document the decision of the risk assessment of the retail loan department.

Chapter 3
Other Considerations

The following factors should also be considered while undertaking the risk-based internal audit assignments in banks as per the extant guidelines of RBI:

Functional independence

3.1.1 The internal audit function should be independent from the internal control process in order to avoid any conflict of interest and should be given an appropriate standing within the bank to carry out its assignments. It should not be assigned the responsibility of performing other accounting or operational functions. The management should ensure that the internal audit staff performs their duties with objectivity and impartiality. Normally, the internal audit head (HIA) should report to the Board of Directors through Audit Committee of the Board. Preferably Internal Audit Head should be one level below CEO. HIA shall not have any reporting relationship with the business verticals of Senior Management and shall not be assigned any business target.

3.1.2 The Board of Directors and top management will be responsible for having in place an effective risk-based internal audit system and ensure that its importance is understood throughout the bank. The success of internal audit function depends largely on the extent of reliance placed on it by the management for guiding the bank's operations. 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

3.1.3 In this context, attention is invited to the Auditing and Assurance Standard 7, “Relying Upon the Work of An Internal Auditor” which provides that the general evaluation of the internal audit function will assist the external auditor in determining the extent to which he can place the reliance on the work of internal auditor. The Standard also requires the organizational status

of the internal audit function to be examined as a part of the general evaluation and provides that:

"Whether internal audit is undertaken by an outside agency or by an internal audit department within the entity itself, the internal auditor reports to the management. In an ideal situation, he reports to the highest level of management and is free of any other operating responsibility. Any constraints or restrictions placed upon his work by management should be carefully evaluated."

Communication

3.2 The communication channels between the risk-based internal audit staff and management should 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 Audit Committee or top management, as appropriate. In particular, the internal auditor should be free to communicate fully with the external auditor. All the pending high and medium risk observations 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.

Performance evaluation

3.3 The Internal audit function should conduct periodical reviews, annually or more frequently, of the risk-based internal audit undertaken by it *vis-à-vis* the approved audit plan. The performance review should also include an evaluation of the effectiveness of risk-based internal audit in mitigating identified risks.

The Audit Committee of Board should formulate and Maitain Quality Assurance and Improvement Program to periodically assess the performance of the risk-based internal audit for reliability, accuracy and objectivity. Variations, if any, in the risk profile as revealed by the risk-based internal audit *vis-à-vis* the risk profile as documented in the audit plan should also be looked into to evaluate the reasonableness of risk assessment methodology of the internal audit function. Further ACB / Board shall promote the use of new audit tools / technologies for reducing manual monitoring/ transaction testing etc.

Relationship with the external auditor

3.4 While the external auditor has the final responsibility for the audit report signed by him and for determination of the nature, timing and extent of the auditing procedures, much of the work of the internal audit function may be useful to him in his examination of the financial information. Towards this end, the Auditing and Assurance Standard 7, "Relying Upon The Work Of An Internal Auditor" provides for a framework of relationship between the internal auditor and the external auditor, which should be considered while determining the risk-based audit plan.

Chapter 4
The Way Ahead

Risk-based internal audit is expected to be an aid to the ongoing risk management in banks by providing necessary checks and balances in the system. However, since risk-based internal audit will be a fairly new exercise for most of the Indian banks, a gradual but effective approach would be necessary for its implementation.

In this connection, it is important to note that the ICAI has come out with several audit pronouncements including Guidance Note on Audit of Banks, which will provide guidance on risk assessment and its importance to the audit function. The growing concern of internal controls particularly in a post-Sarbanes Oxley era and its applicability to the banking industry is a professional opportunity for the members of the Institute to contribute to the enterprise-wide risk management initiatives of the banks using the internal audit function.

Further, the risk management perspective of the operations is being given due importance under the proposed Basel International Capital Adequacy framework whereby the banks with increased risk mitigant strategies are rewarded suitably with the lower capital requirements whereas the high risk banks are subject to stringent capital requirements.

Appendices

Reserve Bank of India Circulars on Risk-based Internal Audit

I DBS.CO/RBS/58/36.01.002/2001-02 dated August 13, 2001

II DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002

III DBS.CO.PP.BC.17/11.01.005/2004-05 dated February 1, 2005

IV DoS.CO.PPG./SEC.04/11.01.005/2020-21 dated January 7, 2021

V DoS.CO.PPG./SEC.05/11.01.005/2020-21 dated February 3, 2005

Appendix - I
Move towards Risk based Supervision (RBS) of banks - Discussion Paper

13th August 2001

DBS.CO/ RBS/58/36.01.002/2001-02

All Scheduled Commercial Banks
(Except Regional Rural Banks)

Dear Sirs,

Please refer to paragraph 76 of our Governor's statement on 'Monetary and Credit Policy for the year 2000-2001' wherein it has been stated that the Reserve Bank would be developing an overall plan for moving towards Risk-based Supervision (RBS) with the assistance of international consultants. Accordingly, Price water house Coopers (PwC), a firm of consultants based in London, were engaged to undertake a review of the current regulatory and supervisory regime and prepare the blue print for the transition to a more sophisticated system of RBS incorporating international best practices. A discussion paper on the 'Move towards Risk-based Supervision of banks' has been prepared summarizing the recommendations of the consultants and is enclosed.

2. It may be observed from the discussion paper that the Reserve Bank would focus its supervisory attention on the banks in accordance with the risk each bank poses to itself as well as to the system. The risk profile of each bank would determine the supervisory programme comprising off-site surveillance, targeted on-site inspections, structured meetings with banks, commissioned external audits, specific supervisory directions and new policy notices in conjunction with close monitoring through a Monitorable Action Plan (MAP) followed by enforcement action, as warranted. The successful implementation of the process of RBS entails adequate preparation, both on the part of the Reserve Bank and the commercial banks.

3. The introduction of RBS would require the banks to reorient their organisational set up towards RBS and put in place an efficient risk management architecture, adopt risk focused internal audit, strengthen the management information system, and set up compliance units. The banks would also be required to address HRD issues like manpower planning, selection and deployment of staff and their training in risk management and risk based audit. It is evident that change management is a key element in

RBS and the banks should have clearly defined standards of corporate governance, well documented policies and efficient practices in place so as to clearly demarcate the lines of responsibility and accountability so that they align themselves to meet the requirements of RBS.

4. The discussion paper may please be placed before the Board of Directors for deliberation in the next meeting. The comments of the bank on the various aspects of the discussion paper may please be forwarded to us as early as possible but before September 30, 2001.On the basis of the feed back received from the banks further discussions would be held.

5. In the meanwhile, kindly acknowledge receipt.

(A.L.Narasimhan)

Chief General Manager-in-charge

Encl: Discussion paper on "Move towards risk based Supervision of banks"

Reserve Bank of India
Department of Banking Supervision - Central Office
Move towards Risk-based Supervision of Banks – A Discussion Paper

Part I
Background

1. The international banking scene has in recent years witnessed strong trends towards globalization and consolidation of the financial system. Stability of the financial system has become the central challenge to bank regulators and supervisors throughout the world. The multi-lateral initiatives leading to evolution of international standards and codes and evaluation of adherence thereto represent resolute attempts to address this challenge.

2. The Indian banking scene has witnessed progressive deregulation, institution of prudential norm and an emulation of international supervisory best practices. The supervisory processes have also concomitantly evolved and have acquired a certain level of robustness and sophistication with the adoption of the CAMELS1/CALCS2 approach to supervisory risk assessments and rating. The tightening of exposure and prudential norms and enhancement in disclosure standards in phases over a period of time have more closely aligned the Indian banking system to international best practices. Reserve

Bank of India (RBI) has been constantly endeavouring to enhance the sophistication and efficiency levels of its supervisory processes.

3. The announcement made by the Governor, RBI, as part of the monetary and credit policy statement for 2000-2001 that RBI would be developing an overall plan for moving towards risk- based supervision (RBS) with the assistance of international consultants signified the launch of a new initiative in this direction. Pricewaterhouse Coopers (PWC) based in London, were selected to undertake a review of the current regulatory and supervisory processes of the RBI with a view to assisting in the introduction of risk based regulation and supervision in India. The RBS will be a regime in which RBI's resources will be directed towards the areas of greater risk to its supervisory objectives. There are two legs to implementing effective risk-based processes: first, explicit supervisory objectives must be set and secondly, the risks posed to these objectives by the activities of commercial banks must be assessed and addressed. The current review represents further stage in the overall development of RBI's approach to regulating and supervising banks in the light of the earlier Padmanabhan Committee and Narasimham Committee reports. Based on the work of the international consultants, RBI intends to move towards a RBS system in stages.

Current approach

4. The current supervisory process adopted by the Department of Banking Supervision (DBS) is applied uniformly to all supervised institutions. Though scrutiny of systems and procedures prevailing in supervised institution is an integral part of on-site inspection, there is scope for more focus on the risk profile of the institutions. The current approach is largely on-site inspection driven supplemented by off-site monitoring and the supervisory follow-up commences with the detailed findings of annual financial inspection. The process is based on CAMELS/CALCS approach where capital adequacy, asset quality, management aspects, earnings, liquidity and systems and control are examined keeping in view the requirements of Section 22 of the Banking Regulation Act, 1949. The on-site inspections are conducted, to a large extent with reference to the audited balance sheet dates. The off-site and market intelligence play a supplemental role. While in several external jurisdictions, the supervisory process extensively leverages on the work done by others, such as the internal and external auditors, the use made of these resources in India is rather limited. No legal framework exists for the external auditors to report to the supervisor their adverse findings on issues having supervisory implications.

Risk-based supervision - A New approach

5. Considering the growing diversities and complexities of banking business, the spate of product innovation with complex risk phenomena, the contagion effects that a crisis can spread and the consequential pressures on supervisory resources, the RBS approach, the foundation of which would be based on the CAMELS based approach, would be more appropriate. By optimizing the synergies from the different activities, including the regulatory and supervisory functions, the overall efficiency and effectiveness of the supervisory process can be substantially enhanced.

Objectives of RBS

6. The RBS approach essentially entails the allocation of supervisory resources and paying supervisory attention in accordance with the risk profile of each institution. The approach is expected to optimize utilisation of supervisory resources and minimize the impact of crisis situation in the financial system. The RBS process essentially involves continuous monitoring and evaluation of the risk profiles of the supervised institutions in relation to their business strategy and exposures. This assessment will be facilitated by the construction of a Risk matrix for each institution.

7. The instruments of RBS will be by way of enhancement as well as refining of the supervisory tools over those traditionally employed under the CAMELS approach viz. on-site examination and off-site monitoring. The RBS processes and the outcome will be forward looking beyond focusing attention on the rectification of deficiencies with reference to the on-site inspection date. The extent of on-site inspection would be largely determined by the quality and reliability of off-site data, and the reliability of the risk profile built up by banks. The effectiveness of the RBS would clearly depend on banks' preparedness in certain critical areas, such as quality and reliability of data, soundness of systems and technology, appropriateness of risk control mechanism, supporting human resources and organisational back-up.

Supervision process

The major elements of RBS approach are set out below:

Risk profiling of banks

8. The central plank for RBS is an accurate risk profiling for each bank. The risk profile would be a document, which would contain various kinds of financial and non-financial risks faced by a banking institution. The risk assessment would entail the identification of financial activities in which a bank has chosen to engage and the determination of the types and quantities of

risks to which these activities expose the banking institution. The type of risk that banking institution face individually or in combination include, but are not limited to, credit, market, liquidity, operational, legal and reputational risks. The quantity of risks associated with a given activity may be assessed by the volume of assets and the off-balance sheet items that the activity represents or the portion of revenue derived from that activity. Activities that are new to an institution or for which exposure is not readily quantifiable may also represent high risk to an institution that would also be evaluated and included in the risk profile document. The risk profile will also be designed to provide a systematic assessment from the supervisor's perspective of the adequacy and effectiveness of the bank's organisation, management and controls. The main risk-profiling device at present is the CAMELS rating based on on-site inspection, which in course of time will be derived from off-site returns and other information. CAMELS rating would continue to be the core of risk profile compilation, but the successive ratings would be used to reflect trends in contrast to being used as a static annual indicator of risk.

9. The risk profile of each bank will draw upon a wide range of sources of information, besides CAMELS rating, such as, off-site surveillance and monitoring (OSMOS) data, market intelligence reports, ad-hoc data from external and internal auditors, information from other domestic and overseas supervisors, on-site findings, sanctions applied etc. The data inputs would be assessed for its significance and quality before being fed into the risk profile. All outliers i.e. banks which fall outside the normal distribution based on characteristics such as profitability, new business activity, balance sheet growth etc. would be identified on the basis of a two-tailed test (i.e. too good or too bad) and investigated on a regular basis. The risk profile would be constantly updated.

10. The key components of the risk profile document would be the following:
CAMELS rating with trends

- Narrative description of key risk features captured under each CAMELS component
- Summary of key business risks including volatility of trends in key business risk factors
- Monitorable action plan and bank’s progress to date
- Strength, Weaknesses, Opportunities, Threats (SWOT) analysis
- Sensitivity analysis.

RBI would undertake a formal assessment of the risk profile of each bank on a regular basis. The period between assessments would vary depending on the materiality of the risk profile of a bank, with an average period of one year. However, more frequent assessments would be resorted to for higher risk banks and less frequent assessment for lower risk banks.

Supervisory cycle

11. The supervisory process would commence with the preparation of the bank risk profile (based on data furnished by banks to the DBS of RBI, besides data from other sources). The supervision cycle will vary according to risk profile of each bank, the principle being the higher the risk the shorter will be the cycle. The supervision cycle will remain at 12 months in the short-term and will be extended beyond 12 months for low risk banks at a suitable stage. In cases where more frequent application of supervisory process will be necessary, the cycle could even be lesser than 12 months.

Supervisory programme

12. RBI would prepare a bank specific supervisory programme which will set out the detailed work plan for the bank. The scope and objectives of the inspection programme will derive from analysis of risk profile. The supervisory programme would be tailored to individual banks and would focus on the highest risk areas as well as specify the need for further investigation in identified problem areas. The supervisory programme would be prepared at the beginning of the supervisory cycle and would yet be flexible enough to permit amendments warranted by subsequent major developments. The supervisory programme would also identify the package of supervisory tools to be deployed from a range consisting of:

- greater off-site surveillance
- targeted on-site inspection
- structured meetings with banks
- commissioned external audits
- specific supervisory directions
- new policy notices (i.e. new policy directions to banks emanating from individual bank level concerns which are relevant for the industry).

On-site inspection would be largely targeted to specific areas unless a full scope inspection is warranted as per the bank-specific supervisory progamme. A monitorable action plan (MAP), the details of which are given later, to

mitigate risks to supervisory objectives posed by individual banks would be drawn up for follow-up. Variable supervisory cycles and variable frequency of inspections would therefore characterise the supervisory process under RBS.

Inspection process

13. The risk assessment of individual banks would be performed in advance of on-site supervisory activities. The risk assessment process would highlight both the strengths and vulnerabilities of an institution and would provide a foundation from which to determine the procedures to be conducted during the inspection. The current full-scope on-site inspections, which are carried out annually cover a substantive asset evaluation. The inspections under the new approach would be largely systems based rather than laying emphasis on underlying transactions and asset valuations. The inspection would target identified high-risk areas from the supervisory perspective and would focus on the effectiveness of mechanism in capturing, measuring, monitoring and controlling various risks. The inspection procedure would continue to include transaction testing and evaluation the extent of which will depend on the materiality of an activity and the integrity of the risk management system and the control process.

Review, evaluation and follow-up

14. An evaluation will be undertaken to ensure that the supervisory programme has indeed been completed and been effective in improving the risk profile of the bank concerned. If need be, further tools will be employed including additional inspection visits. The findings of inspection and other supervisory information on records would be used to produce a comprehensive document of supervisory risks and the bank's assigned ratings for follow-up of supervisory concerns. The risk profile document of the bank will accordingly be updated in the light of new information. This process will support the issue of the supervisory letter to the bank, which would be discussed with the bank's management or the Board of Directors.

Monitorable action plan

15. The aim of supervisory follow-up would be to ensure that banks take corrective action in time to remedy or mitigate any significant risks that have been identified during the supervisory process. The major device in this respect would be the MAP. MAPs are already used by RBI to set out the improvements required in the areas identified during the current on-site and off-site supervisory process. However, MAPs would be made more robust in a number of ways. MAPs will in many cases include directions to banks on

actions to be taken. The remedial actions that would be outlined, would be tied explicitly to the areas of high risks identified in the risk profiling as well as the supervisory process and should lead to improvements in the systems and controls environment at the bank. Key individuals at the bank would have to be made accountable for each of the action points. If actions and timetable set out in the MAP are not met, RBI would consider issuing further directions to the defaulting banks and even impose sanctions and penalties.

Supervisory organisation

16. Within the RBI, the regulatory and supervisory structure function separately at present making it necessary for banks to have more than one contact point with the RBI Regulation (DBOD) and Supervision (DBS) departments for their interaction on supervisory and regulatory issues. As the bank specific issues would be with reference to the broad regulatory framework in place, a Central Point of Contact in RBI would be of convenience to banks. Under the RBS, there would be a focal point for all contacts by banks both at the Central Office of RBI and its ROs, in respect of all matters relating to regulatory/supervisory issues. This focal point would be the main conduit for information and communication between the banks and RBI.

Enforcement process and incentive framework

17. While the aim of supervisory follow-up is to ensure that banks take corrective action to mitigate significant risks, the persistence of deficiencies would pose a risk to RBI's supervisory objectives. A system of incentives and disincentives has been contemplated under the RBS to better serve attainment of these objectives. Banks with a better compliance record and a good risk management and control system could be entitled to an incentive package which could be in the form of longer supervisory cycle and lesser supervisory intervention. The banks, which fail to show improvement in response to the MAP, would be subjected to a disincentive package such as, more frequent supervisory examination and higher supervisory intervention including directions, sanctions and penalties. The mandatory and discretionary actions as enshrined in the Prompt Corrective Action (PCA) framework would be a part of the supervisory enforcement action. The enforcement function would be carried out through an independent Enforcement Cell to be set up at the BSD to ensure consistency of treatment, maintain objectivity and neutrality of enforcement action.

Role of external auditors in banking supervision

18. The use of specialist third parties, such as, external auditors can be of significant aid to the bank supervisors. In some countries, external auditors are required to perform an early warning function and inform supervisors without delay of information material to the supervisor. The Basel consultative paper 'Internal audit in banks and the relationship of the supervisory authorities with internal and external auditors' discusses the commonality of focus and concern of external auditors and bank supervisors. The supervisory process instead of duplicating the efforts of the external and internal auditors in some areas should seek to leverage off the work done by these agencies. Towards part achievement of this goal, the LFAR format, which is currently under revision, will have to be brought into use at the earliest. RBI would look forward to make more use of external auditors as a supervisory tool by widening the range of tasks and activities which external auditors perform at present. RBI would enter into dialogue with the Institute of Chartered Accountants of India and the bank management to chalk out an action plan.

Change management implications

19. Change management is a key element in ensuring that switchover to RBS takes place in an orderly and effective manner. Banks should have clearly defined standards of corporate governance and documented policies and practices in place so as to clearly demarcate the lines of responsibility and accountability. They will have to address several organisational issues to realign themselves to meet the requirements of RBS. The details of actions that need to be taken by banks are enumerated in Part II.

Part II

20. Bank level preparations

(a) Setting up of risk management architecture

With the progressive deregulation of the financial system as also to address systemic concerns on the safety and soundness of the banking system, RBI advised banks in India in February 1999 to introduce, effective from April 1, 1999, a scientific system of Asset- Liability Management. RBI also issued in October 1999 comprehensive guidelines for putting in place an effective and comprehensive Risk Management System. The guidelines envisaged that banks would set up proper organizational structure, policies, procedures, limits for credit, market and operational risk management. Under the ALM guidelines banks were expected to cover 100% of their assets and liabilities by April 1, 2000. A review undertaken by RBI has revealed that most of the banks are yet

to cover 100 per cent of their assets and liabilities for ALM or set up proper risk management systems and policies for managing credit, market, operational and other risks.

As stated earlier in paragraph 13, supervisory resources would be focused on the areas of higher risks to a bank. The risk profile would highlight both the strengths and vulnerabilities of a bank and would provide a foundation from which to determine the procedures to be conducted during an on-site examination. Under a risk-focused on-site examination approach, the degree of transaction testing would be reduced when internal risk management processes are determined to be adequate or risks are considered minimal. When, however, risk management processes or internal controls are considered inappropriate, additional transaction testing sufficient to fully assess the degree of risk exposure in a function or activity would be performed. It would be necessary for banks to carry out a fresh review of their current status of risk management architecture by an expert team and initiate measures to bridge the gaps.

(b) Adoption of risk focused internal audit

Internal Audit is an independent activity designed to improve the bank's operations. The internal audit function is a part of the ongoing monitoring of the system of internal control and assists the staff in effective discharge of their responsibilities. The success of internal audit function depends largely on the extent of reliance the bank management would place in guiding the bank's operations. The Internal Audit Department will therefore have to be independent from the internal control process and be given an appropriate standing within the bank to carry out its assignments with objectivity and impartiality. The Internal Audit Department should therefore be provided with appropriate resources and staff to achieve its objectives. Historically, the internal audit system in banks has been concentrating on: (i) transaction testing, accuracy and reliability of accounting records and financial reports, (ii) testing of integrity, reliability and timeliness of control report, and (iii) adherance to legal and regulatory requirements. Though transaction testing would remain a reliable and essential examination aspect of internal auditing, in the changing scenario such testing by itself would not be sufficient. Over the years, the evolvement of financial instruments and markets have enabled banks to reposition their portfolio risk exposure. It has become clear that periodic assessment based on transaction testing alone cannot keep pace with the rapid changes occurring in financial risk profiles. In this context the widening of the scope of internal auditing assumes significance. The internal

audit would have to capture in a larger way the application and effectiveness of risk management procedures and risk assessment methodology and critical evaluation of the adequacy and effectiveness of the internal control systems. The internal audit department should pay special attention to auditing the banking activity in all the places through which the activity is undertaken. The precise scope of work of internal auditing must be determined by each bank but as a minimum, must review and report upon the control environment as a whole, the process by which risks are identified, analysed and managed, the line of controls over key processes, the reliability and integrity of corporate management function, safeguarding of assets and compliance with rules and regulations.

To achieve these objectives, banks would have to gradually move towards risk focused auditing, in addition to the system of selective transaction based auditing. The implementation of risk based auditing would mean that greater emphasis is placed on the internal auditor's role of mitigating risks. By focussing on effective risk management the internal auditor would not only offer remedies for current trouble areas but also anticipate problems and play an important role in protecting the bank from risk hazards. The Risk based auditing would not only cover assessment of risks at the branch level but would also cover, as an independent assessing authority, assessment of risks at the corporate level and the overall process in place to identify, measure, monitor and control the risks. In order to focus attention on areas of greater risk to the bank, a location-wise and activity-wise risk assessment should be performed in advance of on- site Risk based auditing. This would allow identification of high risk areas which would enable prioritising the activities and locations for Risk based audit. If initial inquiries into the risk management system raise material doubt as to the system's effectiveness, no significant reliance should be placed on the system and a more extensive series of tests need to be undertaken to ensure that the bank's exposure to risk from a given function or activity is accurately captured and monitored. The high-risk areas need to be looked into more frequently than the low risk areas. Risk based audit would be an aid to the ongoing risk management by banks, as it would provide checks and balances in the system. The banks could form a small Committee of executives and entrust them with the responsibility to chalk out an action plan, implement and monitor the progress in adoption of risk management systems and risk focused audit and report to the Top Management and Board of Directors periodically.

(c) Strengthening of Management Information System and Information Technology

A principal foundation for RBS is the availability of detailed data. Under RBS the monitoring needs of RBI will differ based on the risk profile of a bank and accordingly RBI may require banks to provide information in addition to the data now being furnished in the OSMOS returns. Consequently, there is a need to devise a policy for backup and storage of various databases on regular intervals. The policy should specify details like frequency of backups, media to be used, off-site storage areas, departments and officials (Data Managers) responsible for these actions. The accuracy, completeness and the timeliness of data are very important and would have to be ensured by banks through up-gradation of their management information and information technology systems. The Data Manager's role should be created in order to ensure that the data has integrity, is stored in correct place, comprehensive and timely. The Data Managers should be made responsible for specific databases. Banks should review the present status of the management information and information technology systems and initiate necessary measures to ensure that RBI data needs as well as supervisory reporting systems are streamlined.

(d) Addressing HRD issues

A major transitional task towards completion of risk management set up and introduction of Risk based audit will be the reorientation of the staff to meet the required objectives. The potential primary obstacles will be the skill formation of the staff and placement in appropriate positions. Banks may have to create a dedicated risk management team at head office and reorient the Internal Audit Department to undertake risk-based audit. These objectives could be attained through addressing several HRD issues like manpower planning, selection and deployment of staff and extensive training in risk management including asset liability management and Risk based audit. The banks will have to adopt a forward looking training arrangement through appropriate course designing and compilation of training materials keeping in view the best international practices and procedures.

(e) Setting up of Compliance Unit

Banks are required to take corrective action to remedy or mitigate any significant risks which have been identified in the earlier part of the supervisory cycle and which have been incorporated into the current risk profile. RBI will issue bank specific MAP which will include directions to banks on actions to be taken. If the actions and timetable set out in the MAP fail to be met, RBI may issue further directions or impose sanctions or take mandatory and

discretionary actions, if deficiencies continue to persist. It is therefore necessary for banks to set up a dedicated compliance unit to coordinate various actions of the bank for compliance and for periodical reporting to RBI, and ensure the completion of compliance action within the time period indicated in the MAP. The compliance unit should be headed by a Chief Compliance Officer of the rank of not less than a General Manager who will be responsible and accountable for timeliness and accuracy of the compliance.

Part III

Implementation Schedule

21. The major transitional task would be the reorientation of organizational set up by banks in line with the recommendations for bank level preparation. The main obstacle during the transitional period would be skill formation, attitudinal changes, development and retention of specialist staff, extensive training and redeployment of staff. It is not contemplated to change over to RBS approach in one go. It will be implemented in a gradual manner. However, the shift to RBS approach would not necessarily await the completion of bank level preparation. The concept is intended to be rolled out at the earliest, as the inadequacies in risk management systems in banks will themselves be a supervisory risk. As the CAMELS rating would be an important input in bank risk profiling, the CAMELS approach through on-site inspection would concurrently be followed along with the RBS approach in the shorter term. The procedure would be reviewed at the appropriate time in the light of the quality of Management Information System in banks and the accuracy and completeness of relevant off-site data furnished to the BSD of RBI which would then form the basis for compilation of CAMELS rating. At that stage, the on-site inspection for CAMELS rating would be by way of exception.

22. It is intended to roll out the RBS process in phases beginning from the last quarter of the financial year 2002-2003. It is, therefore, necessary for banks to initiate immediate measures for completion of the tasks indicated in paragraph 21 of this document by the end of the calendar year 2002. Banks may like to set up an in-house change management team to monitor the progress of implementation and suggest ways and means to overcome the obstacles.

1. Capital adequacy, Asset quality, Management, Earnings,Liquidity, Systems and control. (applicable to all domestic banks)

2. Capital adequacy, Asset quality, Liquidity, Compliance and Systems. (applicable to Indian operations of banks incorporated outside India)

Appendix - II
Risk-based Internal Audit

DBS.CO.PP.BC . 10 /11.01.005/2002-03

December 27, 2002

All Scheduled Commercial Banks
(Except Regional Rural Banks)

Dear Sirs,

Please refer to Part II of the discussion paper on `Move towards risk-based supervision of banks' forwarded to you vide letter No. DBS. CO. RBS.58/ 36.01.002/ 2001-02 dated August 13, 2001 wherein five areas of bank level preparation had been identified, which will be significant in facilitating a smooth switchover to risk-based supervision (RBS) of banks by the Reserve Bank. One of the areas relate to the introduction of a risk-based internal audit system by banks. The guidelines have now been finalised and the guidance note relating to risk-based internal audit system is enclosed.

2. The guidance note may please be placed before the Board of Directors for deliberation at the next meeting, and banks may immediately initiate necessary steps to review their current internal audit systems and prepare for transition to a risk-based internal audit system in a phased manner, keeping in view their risk management practices, business requirements, manpower availability, etc.

3. Banks should form a Task Force comprising senior executives and entrust them with the responsibility of chalking out an action plan for switching over to risk-based internal audit. The task force may identify and address transitional and change management issues, implement the action plan, monitor the progress in the transitional period and report periodically to the Board of Directors and Top Management. A quarterly report beginning from the quarter ending March 31, 2003 on the progress made in implementation of risk based internal audit may be submitted to us as also to the Regional Office of Department of Banking Supervision under whose jurisdiction the Head Office of the bank is situated.

4. Kindly acknowledge receipt.

Yours faithfully,

Sd/-

(P. V. Subba Rao)

Chief General Manager-in Charge

Encl: Guidance note on risk-based internal audit

Annexure
Guidance Note on Risk-based Internal Audit

1. Introduction

1.1. The evolvement of financial instruments and markets has enabled banks to undertake varied risk exposures. In the context of these developments and the progressive deregulation and liberalisation of the Indian financial sector, having in place effective risk management and internal control systems has become crucial to the conduct of banking business. This is also significant in view of proposed introduction of the New Basel Capital Accord under which capital maintained by a bank will be more closely aligned to the risks undertaken and Reserve Bank's proposed move towards risk-based supervision (RBS) of banks. Under the proposed RBS approach, the supervisory process would seek to leverage the work done by internal auditors of banks. In this regard, the discussion paper on `Move towards risk-based supervision of banks' dated August 13, 2001 may be referred. Part II of the discussion paper clearly identifies five significant areas for action on the part of banks, including putting in place risk-based internal audit system by December 2002, to facilitate a smooth switchover to RBS.

1.2. A sound internal audit function plays an important role in contributing to the effectiveness of the internal control system. The audit function should provide high quality counsel to management on the effectiveness of risk management and internal controls including regulatory compliance by the bank. Historically, the internal audit system in banks has been concentrating on transaction testing, testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, and adherence to legal and regulatory requirements. However, in the changing scenario such testing by itself would not be sufficient. There is a need for widening as well as redirecting the scope of internal audit to evaluate the adequacy and effectiveness of risk management procedures and internal control systems in the banks.

1.3. To achieve these objectives, banks will have to gradually move towards risk-based internal audit which will include, in addition to selective transaction testing, an evaluation of the risk management systems and control procedures prevailing in various areas of a bank's operations. The implementation of risk-based internal audit would mean that greater emphasis is placed on the internal auditor's role in mitigating risks. While focusing on effective risk management and controls, in addition to appropriate transaction testing, the risk-based internal audit would not only offer suggestions for mitigating current

risks but also anticipate areas of potential risks and play an important role in protecting the bank from various risks.

1.4 The functions of the Risk Management Committee/Department (RMC/RMD) and the role of risk-based internal audit need to be distinguished. The RMC/RMD focuses on areas such as identification, monitoring and measurement of risks, development of policies and procedures, use of risk management models, etc., as outlined in paragraph 2 of the guidelines on Risk Management systems in Banks enclosed with our circular DBOD No. BP.(SC).BC.98/21.04. 103/99 dated October 7, 1999. The risk-based internal audit, on the other hand, undertakes 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. It needs to be emphasized that while formulating the audit 2 plan, every activity/location of the bank, including the risk management function, should be subjected to risk assessment by the risk- based internal audit.

2. Policy for risk-based internal audit

2.1. Under risk-based internal audit, the focus will shift from the present system of full-scale transaction testing to risk identification, prioritization of audit areas and allocation of audit resources in accordance with the risk assessment. Banks will, therefore, need to develop a well defined policy, duly approved by the Board, for undertaking risk-based internal audit. The policy should include the risk assessment methodology for identifying the risk areas based on which the audit plan would be formulated. The policy should also lay down the maximum time period beyond which even the low risk business activities/locations should not remain unaudited.

3. Functional independence

3.1. The Internal Audit Department should be independent from the internal control process in order to avoid any conflict of interest and should be given an appropriate standing within the bank to carry out its assignments. It should not be assigned the responsibility of performing other accounting or operational functions. The management should ensure that the internal audit staff perform their duties with objectivity and impartiality. Normally, the internal audit head should report to the Board of Directors/Audit Committee of the Board1.

3.2. The Board of Directors2 and top management will be responsible for having in place an effective risk-based internal audit system and ensure that

its importance is understood throughout the bank. The success of internal audit function depends largely on the extent of reliance placed on it by the management for guiding the bank's operations.

4. Risk assessment

4.1. As indicated at paragraph 1.4 above, the risk-based internal audit undertakes risk assessment solely for the purpose of formulating the risk-based audit plan. The risk assessment would, 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. The internal audit department should devise the risk assessment methodology, with the approval of the Board of Directors, keeping in view the size and complexity of the business undertaken by the bank.

4.2. The risk assessment process should, inter alia, include the following :-

- Identification of inherent business risks in various activities undertaken by the bank.
- ·Evaluation of the effectiveness of the control systems for monitoring the inherent risks of the business activities (`Control risk').
- ·Drawing up a risk-matrix for taking into account both the factors viz., inherent business risks and control risks. An illustrative risk-matrix is shown as a box item.
- 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. In order to focus attention on areas of 3 greater risk to the bank, an activity-wise and location-wise identification of risk should be undertaken.

The risk assessment methodology should include, inter alia, the following parameters:

- Previous internal audit reports and compliance
- Proposed changes in business lines or change in focus
- Significant change in management / key personnel

- Results of latest regulatory examination report
- Reports of external auditors
- Industry trends and other environmental factors
- Time lapsed since last audit
- Volume of business and complexity of activities
- Substantial performance variations from the budget

4.3. For the risk assessment to be accurate, it will be necessary to have in place proper MIS and data integrity. 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.

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 banks 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, these areas would 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 should be prepared for each business activity/ location.

4.4 All banks need to put in place an independent risk assessment system in the internal audit department for focusing on the material risk areas and prioritizing 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.

5. Audit Plan

5.1. The annual audit plan, approved by the Board, should include the schedule and the rationale for audit work planned. It should also 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 regulatory guidelines, as applicable.

6. Scope

6.1. The primary focus of risk-based internal audit will be to provide reasonable assurance to the Board and top management about the adequacy and effectiveness of the risk management and control framework in the banks' operations. While examining the effectiveness of control framework, the risk-based internal audit should report on proper recording and reporting of major

exceptions and excesses. Transaction testing would continue to remain an essential aspect of risk-based internal audit. The extent of transaction testing will have to be determined based on the risk assessment. Illustratively, the bank should 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 banks may also consider transaction5 testing with an element of surprise in respect of low risk areas which would be audited at relatively longer intervals.

The banks may prepare a Risk Audit Matrix as shown below:

Risk Audit Matrix

The Audit Plan should prioritize audit work to give greater attention to the areas of:

i. High Magnitude and high frequency

ii. High Magnitude and medium frequency

iii. Medium magnitude and high frequency

iv. High magnitude and low frequency

v. Medium Magnitude and medium frequency.

6.2. The precise scope of risk-based internal audit must be determined by each bank for low, medium, high, very high and extremely high risk areas. However, at the minimum, it must review/report on:-

- process by which risks are identified and managed in various areas;
- the control environment in various areas;
- gaps, if any, in control mechanism which might lead to frauds, identification of fraud prone areas;
- data integrity, reliability and integrity of MIS;
- internal, regulatory and statutory compliance;
- budgetary control and performance reviews;
- transaction testing/verification of assets to the extent considered necessary
- monitoring compliance with the risk-based internal audit report
- variation, if any, in the assessment of risks under the audit plan vis-à-vis the riskbased internal audit.

6.3. The scope of risk-based internal audit 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.

7. Communication

The communication channels between the risk-based internal audit staff and management should 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 of Directors, Audit Committee or top management, as appropriate.

8. Performance evaluation

8.1. The Internal Audit Department should conduct periodical reviews, annually or more frequently, of the risk-based internal audit undertaken by it vis-à-vis the approved audit plan. The performance review should also include an evaluation of the effectiveness of risk-based internal audit in mitigating identified risks.

8.2. The Board of Directors/Audit Committee of Board should periodically assess The performance of the risk-based internal audit for reliability, accuracy and objectivity. Variations, if any, in the risk profile as revealed by the risk-based internal audit vis-à-vis the risk profile as documented in the audit plan should also be looked into to evaluate the reasonableness of risk assessment methodology of the Internal Audit Department.

9. Audit resources

9.1. The Internal Audit Department should be provided with appropriate resources and staff to achieve its objectives under the risk-based internal audit system. The staff possessing the requisite skills should be assigned the job of undertaking risk-based internal audit. They should also be trained periodically to enable them to understand the bank's business activities, operating procedures, risk management and control systems, MIS, etc.

10. Outsourced internal audit arrangements

10.1 The Board of Directors and top management are responsible for ensuring that the risk-based internal audit continues to function effectively even though it is outsourced.

The following aspects may, inter-alia, be kept in view to prevent any risk of breakdown in internal controls on account of outsourcing arrangements:-

a. Before entering into an outsourcing arrangement for risk-based internal audit, the bank should 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:

- the scope and frequency of work to be performed by the vendor
- the manner and frequency of reporting to the bank the manner of determining the cost of damages arising from errors, omissions and negligence on the part of the vendor
- the arrangements for incorporation of changes in the terms of contract, should the need arise
- the locations where the work papers will be stored
- the internal audit reports are the property of the bank and that all work papers are to be provided to the bank when required
- the employees authorized by the bank are to have reasonable and timely access to the work papers
- the supervisors are to be granted immediate and full access to related work papers

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

c. All work done by the vendor should be documented and reported to the top management through the internal audit department.

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

11. Risk-based internal audit is expected to be an aid to the ongoing risk management in banks by providing necessary checks and balances in the system. However, since risk based internal audit will be a fairly new exercise for most of the Indian banks, a gradual but effective approach would be necessary for its implementation. Initially the risk-based internal audit may be used as a management/audit tool in addition to the existing internal audit/inspection. Once the risk- based internal audit stabilizes and the staff

attains proficiency, it should replace the existing internal audit/inspection. The information systems audit (IS Audit) should also be carried out using the risk-based approach.

12. Banks should form a Task Force of senior executives and entrust them with the responsibility to chalk out an action plan for switching over to risk-based internal audit, identifying and addressing transitional and change management issues, implementing the plan and monitoring the progress during the transitional period and report to the Board of Directors, periodically.

1. In case of foreign banks the reporting could be to the CEO for Indian operations.
2. In this document the expression Board/Audit Committee of Board should be taken to mean the Local Advisory Board in case of foreign banks, unless otherwise specified.

Appendix - III
RESERVE BANK OF INDIA

www.rbi.org.in

Implementation of Risk-based Internal Audit (RBIA) in Banks

Ref. RBI 2004-05 /356

DBS.CO.PP.BC.17/11.01.005/2004-05 February 1, 2005

All Scheduled Commercial Banks

(Except Regional Rural Banks)

Dear Sirs,

As you would recall the guidelines relating to risk-based internal audit were issued by us on December 27, 2002 vide our letter DBS.CO.PP.BC.10 /11.01.005/2002-03. A review of the implementation of the risk-based internal audit in various banks has revealed that there are certain gaps/deficiencies which need to be addressed in order to ensure that the RBIA framework is effective. Some of the gaps/deficiencies observed by us are as under:

1) The risk assessment of branches should be carried out on the basis of the “inherent business risks” and “control risks”, as indicated in paragraph 4.2 of our 'Guidance note on risk based internal audit'.

2) The risk assessment should not only indicate the level of risk as High, Medium and Low but also the trend of risk in terms of increasing, decreasing or stable. (paragraph 4.2 of the 'Guidance note on risk based internal audit'.)

3) The risk assessment should invariably be undertaken on a yearly basis (paragraph 4.3 of the 'Guidance note on risk based internal audit'.)

4) As mentioned in paragraph 6.1 of the 'Guidance note on Risk-based internal audit', the bank should 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 banks may also consider transaction testing with an element of surprise in respect of low risk areas which would be audited at relatively longer intervals. As regards the areas falling in other cells (viz., ‘A-High Risk’, ‘D-Medium Risk’, ‘E-High Risk’, ‘G-Low Risk’, ‘H-Medium Risk’, ‘I-High Risk’) of

the risk matrix, the bank has to decide on the level of transaction testing based on its risk based internal audit policy duly approved by the Board.

5) As indicated in paragraph 6.1 of the 'Guidance note on risk based internal audit', the bank has to prepare a Risk Audit Matrix which would be based on the magnitude and frequency of risk. Preparation of the Risk Audit Matrix can also enable the bank to move towards the Advanced Measurement Approach for Operational Risk under Basel II.

2. Banks are advised to review the methodology of conducting the risk-based internal audit and the policy in this regard so as to align the same with the guidelines issued by RBI. As already indicated in paragraph 3 of our letter dated December 27, 2002, mentioned above, banks should form a Task Force comprising senior executives and entrust them with the responsibility of chalking out an action plan for switching over to risk-based internal audit. This process may be expedited and compliance with our guidelines ensured at an early date.

Yours faithfully,

(Amarendra Mohan)
General Manager

Appendix - IV
RESERVE BANK OF INDIA

www.rbi.org.in

Risk Based Internal Audit (RBIA) Framework – Strengthening Governance arrangements

RBI/2020-21/83

Ref.No.DoS.CO.PPG./SEC.04/11.01.005/2020-21 January 07, 2021

The Chairman / Managing Director / Chief Executive Officer
All Scheduled Commercial Banks (Excluding RRBs) All Local Area Banks
All Small Finance Banks and
All Payments Banks

Madam / Dear Sir,

Risk Based Internal Audit (RBIA) Framework – Strengthening Governance arrangements

In terms of the *Guidance Note on Risk-Based Internal Audit* issued by RBI vide circular DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002, banks, *inter alia,* are required to put in place a risk based internal audit (RBIA) system as part of their internal control framework that relies on a well-defined policy for internal audit, functional independence with sufficient standing and authority within the bank, effective channels of communication, adequate audit resources with sufficient professional competence, among others.

2. While the aforesaid Guidance Note lays out the basic approach for risk based internal audit functions, banks are expected to re-orient their approach, in line with the evolving best practices, as a part of their overall Governance and Internal Control framework. Banks are encouraged to adopt the International Internal Audit standards, like those issued by the Basel Committee on Banking Supervision (BCBS) and the Institute of Internal Auditors (IIA).

3. To bring uniformity in approach followed by the banks, as also to align the expectations on Internal Audit Function with the best practices, banks are advised as under:

a) Authority, Stature and Independence - The internal audit function must have sufficient authority, stature, independence and resources within the bank, thereby enabling internal auditors to carry out their assignments with objectivity. Accordingly, the Head of Internal Audit (HIA) shall be a senior executive of the bank who shall have the ability to exercise independent judgement. The HIA as well as the internal audit function 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.

b) Competence - Requisite professional competence, knowledge and experience of each internal auditor is essential for the effectiveness of the bank's internal audit function. The desired areas of knowledge and experience may include banking operations, accounting, information technology, data analytics and forensic investigation, among others. Banks should ensure that internal audit function has the requisite skills to audit all areas of the bank.

c) Staff Rotation - 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 departments, so as to have adequate skills for the staff in the Internal Audit function.

d) 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.

e) Reporting Line - The HIA shall directly report to either the Audit Committee of the Board (ACB) / MD & CEO or Whole Time Director (WTD). Should the Board of Directors decide to allow the MD & CEO or a WTD to be the 'reporting authority' of the HIA, then 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. Further, in such cases, the ACB 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 the bank and shall not be given any business

targets. In foreign banks operating in India as branches, the HIA shall report to the internal audit function in the controlling office / head office.

f) 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 that it avoids creating conflict of interest and compromising audit's independence and objectivity.

4. The internal audit function shall not be outsourced. However, where required, experts, including former employees, could be hired 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. Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.

5. Banks must ensure and demonstrate through proper documentation that their risk-based internal audit framework captures all the significant criteria / principles suited for their organisational structure, the business model and the risks.

6. The instructions contained in this circular shall come into effect immediately from the date of this circular.

7. This circular supplement the guidelines issued by Reserve Bank of India on December 27, 2002 on Risk-based internal audit along with other circulars/instruction on the subject issued from time-to time and for any common areas of guidance, the prescription of this circular shall be followed.

Yours faithfully,

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

Appendix - V
RESERVE BANK OF INDIA

www.rbi.org.in

Risk-Based Internal Audit (RBIA)

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

c. All UCBs having asset size of ₹500 crore and above1.

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.

Notes

Notes

ISBN : 81-88437-73-5

Price: ₹ 150/-

BIAMA-006-0124

January | 2024 | P3539 (Revised)

www.icai.org