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

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 Board[1].

3.2. The Board of Directors[2] 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

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.

Risk Matrix

Inherent business risks ↑				
	High	A High Risk	B Very High risk	C Extremely High risk
	Medium	D Medium risk	E High risk	F Very High risk
	Low	G Low risk	H Medium risk	I High Risk
		Low	**Medium**	**High**
		Control Risks →		

Inherent business risks indicate the intrinsic risk in a particular area/activity of the bank and could be grouped into low, medium and high categories depending on the severity of risk.
Control risks arise out of inadequate control systems, deficiencies/gaps and/or likely failures in the existing control processes. The control risks could also be classified into low, medium and high categories.
In the overall risk assessment both the inherent business risks and control risks should be factored in. The overall risk assessment as reflected in each cell of the risk matrix is explained below:

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

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

C – Extremely High Risk – Both the inherent business risk and control risk are high which makes this an Extremely High Risk area. This area would require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring by the bank's top management.

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

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

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

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

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

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

The 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

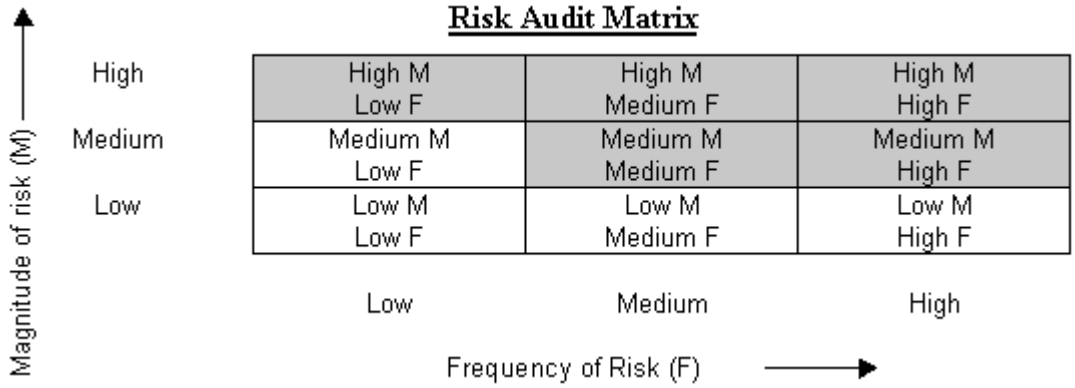
5.1. The annual audit plan, approved by the Board, should include the schedule and the rationale for audit work planned. It should also include all risk areas and their prioritisation based on the level and direction of risk. Illustratively, the areas or activities identified as high, very high or extremely 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 transaction-

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 risk-based 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

7.1. 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.