

RBI/2006-07/177

November 16, 2006

DBS.PP.BC1/11/01.005/2006-07

The Chairman / CEO  
All Scheduled Commercial Banks (excluding RRBs)

Madam / Dear Sir,

**Compliance function in banks**

A system of 'Compliance Officer' in banks was introduced by Reserve Bank of India in August 1992, based on the recommendations of the Committee on Frauds and Malpractices in Banks (Ghosh Committee). Further guidelines in this regard, and more specifically on the role of the Compliance Officers were issued in March 1995. In 1997, a review of the system of Compliance offices was undertaken wherein, in supersession of earlier guidelines, banks were advised that the General Manager in charge of Audit and Inspection should be designated as the 'Compliance Officer' reporting directly to the CMD and submit a quarterly certificate on compliance (subsequently withdrawn in 2000) with RBI/ GOI instructions.

The compliance function in banks however, has not received the required attention by banks, as a number of instances of non-compliance and lack of proper interpretation of regulatory guidelines are being reported in successive RBI inspection reports. Further, in the absence of a comprehensive compliance structure, policy and manual for addressing compliance risk in most of the banks, compliance processes remain weak and the role of the Compliance Officer has not been an effective instrument for which it was created.

In April 2005, the Basel Committee on Banking Supervision (BCBS) had issued a paper on 'Compliance and the Compliance function in banks', prescribing certain principles aimed at strengthening compliance structure in banks. It was, therefore, decided to call a meeting of Compliance Officers in banks in the month of July, 2005. During the course of deliberations with the compliance officers, which was also addressed by Governor,

Reserve Bank of India, it was decided to set up a working group with participation from the banking industry to review the present system of compliance machinery in banks and to recommend measures for strengthening it. The compliance Group, which also had bank representatives, has since submitted its report. Based on the recommendations of the group, comprehensive guidelines on compliance and the compliance function have been formulated and the same are enclosed. The banks would have to implement the guidelines in consultation with the Audit Committee of the Board.

Comments / suggestions are invited from banks and others within a period of one month from the date of this circular. The comments may be addressed to the CGM-in-Charge, Department of Banking Supervision or faxed to 022- 22180157. [Click here to send comments /suggestions by email.](#)

Yours faithfully,

(G.Gopalakrishna)  
Chief General Manager-in-Charge

## 1. Introduction

1.1 Each bank, will formulate a Compliance Function for their bank. The Compliance Function is for ensuring strict observance of all statutory provisions contained in various legislations such as Banking Regulation Act, Reserve Bank of India Act, Foreign Exchange Management Act, Prevention of Money Laundering Act etc. as well as to ensure observance of other regulatory guidelines issued from time to time; standards and codes prescribed by IBA, FEDAI, FIMMDA etc; and also each bank's internal policies and fair practices code. Compliance laws, rules and standards generally cover matters such as observing proper standards of market conduct, managing conflicts of interest, treating customers fairly, and ensuring the suitability of customer advice. They typically include specific areas such as the prevention of money laundering and terrorist financing, and may extend to tax laws that are relevant to the structuring of banking products or customer advice.

Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank. For the reasons mentioned above, these are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

It shall be the responsibility of bank's Compliance Officer in the bank to assist the top management in managing effectively the compliance risks faced by the bank.

## 2. Compliance Risk

2.1 The Basel Committee on Compliance Function defines Compliance risk as “the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities” (together, “*compliance laws, rules and standards*”).

- 2.2 The compliance area is critically important in identifying, evaluating, and addressing legal and reputational risks. Given the significance of these risks, a strong Group/enterprise-wide compliance program is a necessity for banks. A group/enterprise-wide compliance program helps the bank to look at and across business lines and activities of the organization as a whole and to consider how activities in one area of the firm may affect the legal and reputational risks of other business lines and the entire group/ enterprise.
- 2.3 A group/enterprise-wide compliance program could help management and the board in understanding where the legal and reputational risks in the organization are concentrated, provide comparisons of the level and changing nature of risks, and identify those control processes that most need enhancement. The compliance function must therefore ensure that controls and procedures capture the appropriate information to allow senior management and the board to better perform their risk management functions on a group-wide basis.

### **3. Responsibility of the Board and Senior Management**

Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the board of directors and senior management lead by example.

#### **3.1 Responsibility of the Board of Directors**

The Board would be responsible for ensuring that an appropriate compliance policy is in place in the bank to manage compliance risk and also oversee its implementation. It has to ensure that compliance issues are resolved effectively and expeditiously by senior management with the assistance of compliance staff. If necessary, the Board may delegate these tasks either to the Audit Committee of the Board (ACB) or a specific Board level Committee constituted for the purpose. The Board, ACB or the Board Committee, as the case may be, should review compliance function on a quarterly basis. In order to ensure that the activities of the compliance function are subject to independent review, the compliance function and the audit function of the bank should necessarily be kept separate.

## **3.2 Responsibility of Senior Management**

3.2.1 The bank's senior management would be responsible for establishing a written compliance policy that would contain the basic principles to be followed by the management and staff, and would explain the main process by which compliance risk would be identified and managed through all levels of the organization.

3.2.2 The senior management would ensure that appropriate remedial or disciplinary action is taken if breaches are identified.

3.3.3 Senior management should, with the assistance of the compliance function:

- at least once a year, identify and assess the main compliance risk compliance risk issues facing the bank and the plans to manage them.
- at least once a year a report to the board of directors or a committee of the board on the bank's management of its compliance risk, in such a manner as to assist board members to make an informed judgment on whether the bank is managing its compliance risk effectively; and
- report promptly to the board of directors or a committee of the board on any material compliance failure (e.g. failure that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

## **4. The Compliance Policy**

4.1 A robust Compliance system in a bank should include a well documented Compliance Policy, outlining the compliance philosophy of the bank, role and set up of the Compliance Department, composition of its staff and their specific responsibilities. The policy should be reviewed annually by the Board.

4.2 Broadly, the policy should include the following aspects :

- Setting up of an independent Compliance Department at the Head Office with a senior executive heading it with adequate support staff and specifying its role and responsibilities.

- Compliance structure in controlling offices and branches specifying the role and responsibility of each functionary in the Compliance units.
- Measures to ensure independence of the compliance function - It would be necessary that the remuneration of the compliance functionaries is not related to the business line for which they exercise compliance responsibilities though it could generally be related to the financial performance of the bank as a whole.
- Focus of the compliance on regulatory compliance, statutory compliance, compliance with fair practice codes and other codes prescribed / suggested by self-regulatory organizations, government policies, bank's internal policies and prevention of money laundering and funding of illegal activities.
- Monitoring compliance testing procedure
- Right of the compliance function to have access to information necessary to carry out its responsibilities and conduct investigations of possible breaches of compliance policy.
- Relationship between Chief Compliance Officer and head of other functional departments.
- Mechanism for dissemination of information on regulatory matters among operational staff and periodic updating of operational manuals.
- Approval of all new processes and products by the Compliance Department prior to their introduction.
- Right of the compliance function to freely disclose its findings and views to senior management, Board / ACB or Board Committee.

## **5. The Compliance structure**

- 5.1. Depending on its branch network, size and complexity of the business operations, sophistication of products and services offered etc, every bank should decide on the organizational structure and composition of its Compliance unit.

- 5.2 A Compliance Department having formal status should be set up at the Head Office of the bank, (in the case of foreign bank branches it should be at the bank's Principal Office in India). The compliance department should have an executive or senior staff member of the cadre not less than in the rank of DGM or equivalent designated as Group Compliance Officer or Head of Compliance with overall responsibility for coordinating the identification and management of the bank's compliance risk and supervising the activities of other compliance function staff. The Compliance officer, once appointed cannot be removed by the Chief Executive Officer of the bank, except with the specific approval of the Board of Directors of the bank / Head Office of the bank in the case of foreign banks.
- The Board, Audit Committee of the Board or any other Board Committee as the case may be, should be kept informed of any change in the Chief Compliance Officer as also the reason for the change in the incumbent. The Reserve Bank of India shall also similarly be kept informed of the name of the Chief Compliance Officer as also any change thereof, as and when it takes place.
- 5.3. In the case of larger banks, compliance staff may be located within operating business lines. Internationally active banks (including foreign banks having a presence in India) may also have group and local compliance officers reporting to their own Regional / Global Head while closely working with the local CEO on regulatory / compliance issues.
- 5.4 The Compliance Department should be provided with adequate staff. Further, each Department in the Head Office, controlling offices and branches (and / or Strategic Business Units (SBUs) in the case of certain banks as considered appropriate depending on their business delivery model) should have a Compliance Officer, who would report to the Chief Compliance Officer.
- 5.5. The staff in the Compliance Department at the Head Office as also Compliance Officers at controlling offices and branches / SBUs should primarily focus on

compliance functions. However, in small sized banks with limited branch network, the compliance staff could be assigned some other duties while ensuring that there is no conflict of interest. Under no circumstances, the compliance staff should be assigned audit/inspection duty as it gives rise to serious conflict of interest in view of the fact that all products and processes are expected to be cleared by the Compliance Department and its audit needs to be carried out independently by separate set of staff.

- 5.6 Some banks may wish to organize their compliance function within their operational risk function, as there is a close relationship between compliance risk and certain aspects of operational risk. Others may prefer to have separate compliance and operational risk functions, but establish mechanisms requiring close cooperation between the two functions on compliance matters.
- 5.7 Apart from the basic qualifications, the Compliance staff should preferably have a fair knowledge of law, accountancy and information technology and also adequate practical experience in various business lines and audit/inspection functions to enable them to carry out their duties effectively. In order to keep the compliance staff up-to-date with developments in the areas of banking laws, rules and standards, regular and systematic education and training are required.
- 5.8 They should therefore be adequately trained in new products and services introduced in the banking industry as well as in the areas of corporate governance, risk management, supervisory practices etc.
- 5.9 In some banks, the entire compliance responsibilities may not be carried out by the compliance department. Compliance function staff who reside in operating business units or in local subsidiaries may have a reporting line to operating business unit management or local management. This is not objectionable, provided such staff also have a reporting line through to the head of compliance as regards their compliance responsibilities. In cases where compliance function staff



reside in independent support units (e.g. legal, financial control, risk management), a separate reporting line from staff in these units to the head of compliance may not be necessary. However, these units should co-operate closely with the head of compliance.

- 5.10 In all such cases, there should invariably be an appropriate mechanism for co-ordination among these departments to enable the Chief Compliance Officer to perform the assigned responsibilities effectively.
- 5.11 The Chief Compliance Officer should be the nodal point of contact between the bank and the regulator. Regardless of how the compliance function is organized within a bank, it should be independent and sufficiently resourced, its responsibilities should be clearly specified and its activities should be subject to periodic and independent review.
- 5.12 The compliance function should also attend to the compliance of directions from other regulators (IRDA, SEBI etc) in those cases where the activities of the bank are not limited to the banking sector. For example, a bank which is acting as a corporate agent for distribution of other companies' insurance products may receive direction from IRDA, which should be a part of the compliance function. Further, discomfort conveyed to the bank on any issue by other regulators, should be brought to the notice of the Reserve Bank of India.

## **6. Compliance process and procedures**

- 6.1. The Compliance Department at the Head Office should play the central role in the area of identifying the level of compliance risk in each business line, products and processes and issue instructions to operational functionaries. It should circulate the instances of compliance failures among staff along with preventive instructions at least once a year. Inspection/audit findings should serve as a feedback mechanism for the Compliance Department.
- 6.2 Broadly the Compliance process should involve the following actions:

The Compliance Department should be the focal point for receipt and dissemination of all regulatory and internal guidelines/instructions among all operational departments. It should ensure that

- (a) appropriate instructions get promptly issued within the organization,
- (b) the instructions are actually received at each office, and
- (c) the instructions are implemented.

- 6.3. Banks may consider software-based solutions, provided by reputed vendors, which make available all the regulatory instructions and also provide regular updates.
- 6.4. The Compliance risks in all new products and processes should be thoroughly analyzed and appropriate risk mitigants by way of necessary checks and balances should be put in place before launching. The Chief Compliance Officer must be a signatory to all the existing and new products and the policy / procedure formulation for outsourcing contracts in the bank. He should be a member of the 'new product' committee of the bank and all products should be approved him. All new products should be subjected to intensive monitoring for the first six months of introduction to ensure that the indicative parameters of compliance risk are adequately monitored.
- 6.5. The Compliance Department should serve as a reference point for the bank's staff from operational departments for seeking clarifications/ interpretations of various regulatory and statutory guidelines.
- 6.6. Banks should develop function-wise Compliance Manuals duly approved by the Chief Compliance Officer and provide these to the staff associated with the respective functions.
- 6.7. The Compliance Department should go through all audit/inspection reports and rectification reports regularly to enable it to identify compliance failures in the bank. The Compliance Department should, at frequent intervals, interact with Legal Department, Operational risk management Department, Taxation

Department and Audit/Inspection Department of the bank to take stock of the latest developments. Compliance officers should have access to all information they require and have the right to conduct investigation and report the findings to the Chief Compliance Officer. The Chief Compliance Officer shall necessarily be a participant in the quarterly informal discussions held with RBI. In case no quarterly meeting is held, he should meet the Chief General Manager, DBS in charge of the concerned bank at Central Office of RBI, once in every quarter of the year, to discuss compliance issues.

- 6.8. The compliance functionary should be looked at as a friend, philosopher and guide by the business units. There should be close co-ordination and partnership between Compliance and Business Operations functions. The interaction may be formalized by making the Chief Compliance Officer a member of the various inter-departmental committees in the bank.
- 6.9. Banks with fully operational core banking solutions should centralize their regulatory reporting at the Compliance Department. In other cases, Compliance Department shall monitor timely submission of regulatory returns by the controlling offices through appropriate mechanism, such as a Monthly Returns Calendar, which may indicate the returns/reports to be submitted by each branch/controlling office and their dates of submission.
- 6.10. Compliance function should use the internal audit and concurrent audit as a feedback mechanism. The Chief Compliance Officer should be an invitee to the meetings of the ACB. All audit reports should be marked to Chief Compliance Officer and similarly, all reviews by compliance department should be marked to internal audit department.
- 6.11. The compliance function should monitor and test compliance by performing sufficient and representative compliance testing and the results of such compliance testing should be reported to the senior management.

- 6.12. It should also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment.
- 6.13. Compliance staff should be empowered to conduct compliance reviews/investigations, whenever required. The authority to use external experts for the purpose of investigation, if required, should be left to the discretion of the Chief Compliance Officer.
- 6.14. The compliance function should be free to report to senior management on any irregularities. Although its normal reporting line should be to senior management, the compliance function should also have the right of direct access to the board of directors or to a committee of the board, bypassing normal reporting lines. Further, it may be useful for the board or a committee of the board to meet with the head of compliance at least annually, as this will help the board or board committee to assess the extent to which the bank is managing its compliance risk effectively. It should have a right to direct access to the board of directors or a committee of the board.
- 6.15. An Annual Report on compliance failures/breaches should be compiled and placed before the Board/ACB/Board Committee and circulated to all the functional heads. Non-compliance of any regulatory guidelines and administrative actions taken against the bank along with corrective steps taken to avoid recurrence of the lapses should be disclosed in the annual report of the banks.
- 6.16. The code of conduct for employees should envisage working towards earning the trust of the society by dealing with customers in a fair manner and conducting business operations consistent with rules and regulations. Due weightage could be given to record of compliance during performance appraisal of staff at various levels. Staff accountability should be examined for all compliance failures.

## **7. The Compliance Programme**

- 7.1 The responsibilities of the compliance function should be carried out under a compliance programme that sets out its planned activities. The compliance programme should be risk-based and subject to oversight by the head of compliance to ensure appropriate coverage across businesses and co-ordination among risk management functions.
- 7.2. The compliance function may have specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer). Periodical reviews of the compliance systems and procedures within the bank and reporting to the Board are essential for maintaining the effectiveness of the compliance function. Banks should carry out an annual compliance risk assessment in order to identify and assess major compliance risks faced by them and prepare a plan to manage the risks. The Annual review should broadly cover the following aspects.
- Compliance failures, if any during the preceding year and consequential losses and regulatory action as also steps taken to avoid recurrence of the same.
  - List of all major regulatory guidelines issued during the preceding year and steps taken by the bank to ensure compliance.
  - Independence of compliance function
  - Scope of compliance procedures and processes,
  - System of internal control to minimize compliance risk.
  - Compliance with fair practices codes and adherence to standards set by self regulatory bodies and accounting standards.
  - Progress in rectification of significant deficiencies pointed out in the internal audit, statutory audit and RBI inspection reports and position of implementation of recommendations made therein.
  - Strategy for the next year including restructuring of compliance department, if necessary, posting/transfer/training of staff.
- 7.3. Apart from the exhaustive annual review, a monthly report on the position of compliance risk may be put up to the senior management/CEO by the Chief Compliance Officer. A brief report on the compliance position may also be placed before the Board/ACB/Board Committee, as the case may be on a quarterly basis.

- 7.4. Instances of all material compliance failures which may attract a significant risk of legal or regulatory sanctions, financial loss or loss of reputation should be reported to the Board/ACB/Board Committee promptly.
- 7.5. The activities of compliance function should be subject to annual review by the internal audit. Compliance risk shall be included in the risk assessment methodology of the internal audit function and the audit programme shall cover the adequacy and effectiveness of the bank's compliance function including testing of controls commensurate with the perceived level of risk.

## **8. Guidance and education**

The compliance function should advise and assist the senior management on compliance laws, rules and standards, including keeping them informed on developments by establishing written guidance to staff on the appropriate implementation of compliance laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

## **9. Cross Border issues**

- 9.1 Banks may choose to carry on business in various jurisdictions for a variety of legitimate reasons. In such cases, it should be ensured that they comply with applicable laws and regulations in all such jurisdictions and that the organization and structure of the compliance function and its responsibilities are consistent with local legal and regulatory requirements. It is for local businesses to ensure that compliance responsibilities specific to each jurisdiction are carried out by individuals with the appropriate local knowledge and expertise, with oversight from the head of compliance in co-operation with the bank's other risk management functions.