IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 21, Issue 7. Ser. V (July. 2019), PP 74-79
www.iosrjournals.org

RFIA – A Glimpse of ORM in Banking

Abirami T
Assistant Manager State Bank of India, Pondicherry.

Abstract: *The banks and other financial services companies are seriously entangled with crumbling asset quality, erosion in bank profitability and depleting status of bank capital. Stock prices of many banks are substantially lower to book values indicating shareholders are shouldering substantial amount of risk of banks portfolio and operations. The imperative to address this crisis is strengthening of risk management systems of banks.*

Over the last few years, the need to manage risks has become recognized as an essential part of good corporate governance practice. This has put organisations under increasing pressure to identify all the business risks they face and to explain how they manage them. In fact, the activities involved in managing risks have been recognised as playing a central and essential role in maintaining a sound system of internal control. This article intends to provide the importance of RFIA and more focusing on Operational Risk Management in banking sector.

Date of Submission: 06-07-2019 Date of acceptance: 23-07-2019

I. RFIA - Risk Focussed Internal Audit

RFIA also in some banks called Risk Based Internal Audit (RBIA) is not about auditing risks but about auditing the management of risk. Its focus is on the processes applied by the management team. Internal auditors need to spend time with managers, discussing and observing the monitoring controls they apply, rather than re-performing controls or other responses, or analysing data for themselves. Internal auditors should behave in a way that reinforces the fundamental principle that management is responsible for managing risks.

RFIA is the cutting edge of internal audit practice. As a result, it is an area that is evolving rapidly and where there is still little consensus about the best way to implement it.

An independent Risk Governance structure is in place for Integrated Risk Management covering Credit, Market, Operational and Group Risks. This framework, visualises empowerment of Business Units at the Operating level, with the technology being the key driver, enabling identification and management of risk at the place of organisation.

Risk Management is perceived as an enabler for business growth and in strategic business planning, by aligning business strategy to the underlying risks. This is achieved by constantly reassessing the interdependencies/interfaces amongst each silo of Risk and Business Functions.

BASEL II IMPLEMENTATION

The Bank, as per RBI Guidelines, has migrated to Basel II as on 31.03.2008. Simultaneously, processes have been set in train for fine-tuning systems & procedures. IT capabilities and Risk Governance structure to meet the requirements of the Advanced Approaches.

Various initiatives such as migration to new Credit Risk Assessment Modes, independent validation of internal ratings and improvement in Loan Data Quality would not only enable conservation of capital but also facilitate smooth migration to Advanced Approach.

The Essence of Rfia

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.

- 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.

- 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. 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.
- 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.
- 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.
- 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.

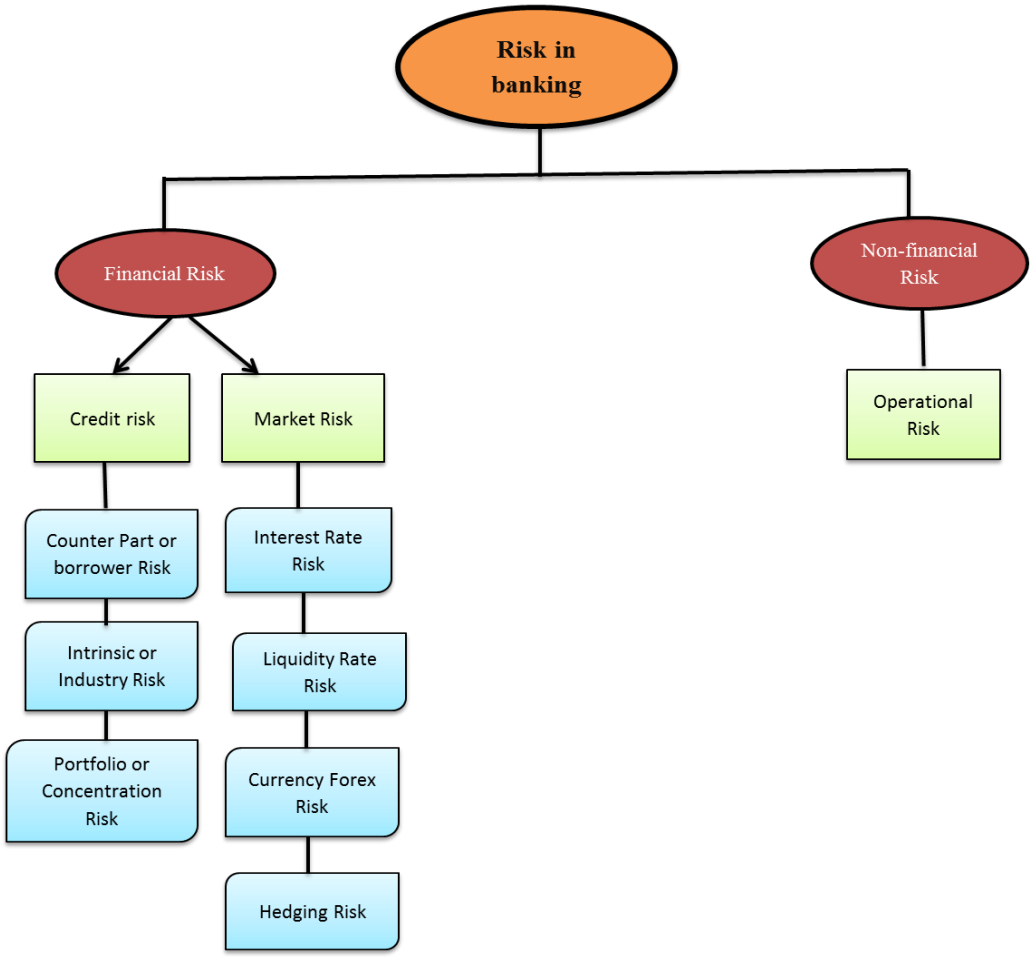
Listed below are some of the benefits of having a good internal audit system in banks:

- Overall operational and control environment of the bank is improved
- Regular internal audit system increases the accountability of the employees
- Strong internal audit process enables early detection of fraud or probable fraud
- Identifies redundant procedures and recommends improvement which increases the operational efficiency
- constant monitoring of the policies and procedures helps in reducing financial risks
- Surprise cash verification by the internal auditors will ensure all the cash transactions are accounted for correctly
- Ensures compliance with statutory law and regulations
- Systematic Internal audit assures the head office that all the banking procedures and rulers are adhered to
- Good control over the bank's non-performing assets
- Regular internal audit at banks gives better comfort and assurance to the statutory auditors too.

Risk Classification

As per Management point of view the Types of Risks in a bank is basically Financial Risks and Non-Financial Risks sub-divided into risks such as:

Market risk
Credit risk
Liquidity risk
Operational risk
Reputation risk
Business and strategic risk



In audit point of view Risk can be classified based on the following criteria:

- Audit of Assets (Operational Risk Management)
- Audit of Liabilities (Credit Risk Management)

The other risks mentioned above are sub-linked to these major audit point of ORM and CRM risks.
As mentioned previously, this article focuses more in ORM.

Operational Risk Management

Operational Risk (non-financial risk) is "the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses.

The study of operational risk is a broad discipline, close to good management and quality management.

In the ORM structure, there are 8 sub-parameters covering 256 modules. Many of these modules are overlapping and placed under one single sub-parameter eg. Business lines is encompassing 93 modules which includes KYC norms, AML Measures, Handling of Pass Books, Handling of Cheque Books, scanning of signatures, Staff Accounts Monitoring, Submission of Account Opening Forms to the Processing Cell etc.

To facilitate correct understanding by the branches, modules have been reorganized. In the revised structure the ORM areas is divided in 25 sub-parameters having 192 modules.

The ORM is not an easy task as the structuring is vast and broad, but if they are established and monitored on regular intervals, it can help in efficient management and better scoring in RFIA.

A summarised position of sub-parameters of revised ORM structure is furnished below:

1. KYC norms
2. AML & CFT Measures
3. Account Opening & Maintenance
4. Collections & Remittances
5. Cheque Issuance, Processing & Payment of Cheques
6. Clearing Module & CTS
7. Handling of Cash

8. Lockers & Safe Custody
9. Alternate Channels
10. Government Business
11. Security Arrangements & Workplace Safety
12. Branch Document & Stationery Records
13. Preventive Vigilance & Controls
14. Recovery of Interest & Charges (Income Leakage)
15. Fraud Monitoring
16. Information Systems Security
17. Customer Service
18. Complaint Management
19. Cross Selling
20. Branch Management & Awareness
21. Personnel
22. Statutory & other General Compliances
23. FATCA & CRS

Of all these parameters, 3 significant parameters are discussed below for sensing the role of a branch head in understanding the importance of ORM and the tasks to be enforced to manage it fruitfully and efficiently.

1. Income Leakage

Income leakage is a drain on the banks profitability and indicates to laxity in controls.

a) Recurrent income leakage has been linked to the audit score
b) Major income heads under which income leakages are being reported at the branches have been identified and a negative score will be assigned to each such head, in the event of recurrent income leakage under that item in the current audit.

The bank fee, unrecovered customers cause loss to the bank, and non-monitoring of the same is described as income leakage.

For instance, Charges for Undelivered & Returned ATM Cards, Cheque Books, Cash Handling Charges, Fee for Articles kept in Safe Deposit, Excess interest paid on deposits etc.

Monitoring of such parameters, not only avoids the losses, but also eradicates the chances of frauds.

2) Handling of Cash

Branch managers need to be aware of the following areas:

- Systems and procedures in cash department
- In branch cash handling procedure
- Clean note policy
- Cash retention limit
- Cash remittance
- Detection of forged notes
- Note refund rules
- Currency Administration cell

The cash and other valuables in a branch will be held in the joint charge of Cash officer and the Branch Manager/Accountant. Cash Officer is responsible for maintenance of the currency chest and functioning of cash department. He is responsible for correctness of the physical cash balance held at the branch as reflected in registers and in system. He should also ensure that all the cashiers/swo receipts and payments are tallied and there is no shortage/excess of cash with them. At the end of the day, he reconciles the physical cash in his possession with the balance reflected in Electronic Cash drawer. The cash officer has to make a surprise check on the operations of the cashiers. Retention limit at the branch is monitored by the cash officer. The clean note policy as per RBI guidelines is followed by him. Detection and impounding Counterfeit Notes should be done as per the norms.

3) Security Arrangement and Workplace Safety

Aide Memoire for Branch Managers is a check list containing the summarised and revised version of the salient aspects of security arrangements at the branches and other entities of the Bank is applicable. This Aide Memoire purports to be a tool in the hands of the Head of Unit to gauge the status of security arrangements of the unit. These may be extraordinary, unique situations and circumstances which may fall beyond the pale of these guidelines and will need to be handled with due reason and circumspection by all concerned to avoid loss of life and property.

This checklist should be made a part of Branch Documents and be handed over from one incumbent to the next.

For best security and safety of the branch, a branch head has to ensure

- ✓ **daily checks, weekly checks, monthly checks, yearly checks –as mentioned below:**

a) locking and closing of rolling shutters, collapsible grills of all entrances of the branch after working hours.
b) All the electrical appliances are switched off before the doors are closed and locked
c) At the time of taking out cash from the strong room, the main gate is closed and locked.
d) The electronic burglar alarm system, automatic fire alarm, CCTV systems are checked and recorded in the daily checking register to confirm that they are functional within the laid down parameter.
e) The cash retention limit fixed for the branch is not exceeded.
f) Surprise inspections of the guards on duty at odd hours/irregular intervals are carried out to ensure/confirm that they are alert. The date & time of such inspections, together with their findings, are recorded in the Guards Inspection Register.
g) Access to System or Server Room should be monitored.
h) The Police Beat Book is verified on regular intervals.
i) The hooters/sirens of the emergency alarm system are functional.
j) The staff members are made aware of the actions to be taken in case of a hold-up, dacoity, fire or any other untoward incident.
k) Inspection of the fire extinguishers is carried out to confirm that refilling is not overdue and that all are in serviceable condition.
l) Anti- termite treatment for strong room, records/stationery room etc is carried out.
m) Liaison with different agencies, viz Police Station, Fire Brigade Station etc. is maintained on continuous basis.
n) The Security Officer visits the branch once a year as laid down. AMC for all security equipment are renewed well in time and the record updated.
o) Branch Contingency, Disaster Recovery and Disaster Management Plans, Emergency Relief Arrangement for the Branch Head/Joint Custodian are prepared and approved by the Controlling Authority.
p) The Duplicate Keys should be deposited at the identified branch and the receipt is on record (not in safe custody/locked up place). And the Duplicate Keys of the branch are withdrawn and verified and redeposited with the link branch on the same day and the details are advised to the Controllers.

Additional Security to be ensured for computer security. Security Precautions during Long Holidays/Weekends.

Rfia – An Inevitable Aspect In Banking.

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.

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, and 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 elapsed since last audit
- Volume of business and complexity of activities
- Substantial performance variations from the budget

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.to implement it. It is more difficult to manage than traditional methodologies.

The risk management framework is a dynamic construction, dependent on people to operate effectively, and it takes continuous effort to keep it working well. As the external environment and the objectives of the organisation change, the circumstances and context of potential risk events also change so that the risk register needs to evolve as time passes.

References

[1]. SBI Role Guide cum Certification Manual.
[2]. RBI Website.

Abirami T" RFIA – A Glimpse of ORM in Banking" IOSR Journal of Business and Management (IOSR-JBM), Vol. 21, No. 7, 2019, pp. -.74-79