Operational Risk Management in Banks - Role of Branches

L. Srinivasan*

Introduction

Banking is defined in Banking Regulations Act 1949, as the acceptance of deposits for the purpose of lending or investment. Later, banks realized that Banking is not as simple as the definition suggests. The South East Asian crisis of the last decade of the 20th century taught banks that Banking is more of Assets-Liability Management (ALM) and also Liquidity Management. Banks understood that they should be able to meet cash and collateral obligations without incurring losses. However, Basel summits and rich experiences have taught banks that Banking can most appropriately be termed as Risk Management. Hence, we may say that Banking operations mean Enterprise-wide Risk Management.

Risks associated with banking functions

Banks today need to manage a host of risks such as liquidity risk, market risk, operational risk, credit risk, foreign exchange risk, sovereign risk and strategic risk. Every bank, especially in our nation, has a dedicated risk management policy, risk management department and risk management committees both at the apex level. Though risks are associated with various banking activities, banks cannot avoid or by-pass risks. Banks have to take risks and manage them. Risk Management has four components- identifying risks, measuring risks, monitoring risks and mitigating risks. When banks do the fine act of balancing risk management and business promotion activities, they will emerge as successful Corporates.

Operational risk management and the role of branches

Among the various risks associated with banks, many are addressed by the Head Office. Virtually, the branches (service outlets) down the line, have little or no role to play in the mitigation of such risks. For example, risks such as market risk, strategic risk, sovereign risk and liquidity risk are studied by teams of researchers at the apex level and mitigation steps are taken. These are spelt out in the Risk Management Policy and are disseminated to the field functionaries.

Perhaps, the only risk where the branch staff-the field functionaries- can actively take part in understanding, monitoring and mitigating, is the operational risk that arises in the normal course of banking business. In fact, every employee in the organization can contribute to the management of operational risk. Let us discuss a few aspects of such operational risk management.

Various operational risk situations/circumstances in day-to-day Banking and their management:

a. *Compliance of KYC norms*: The regulators attach much significance to the total compliance of KYC norms by banks. Getting officially valid documents (OVD) from the prospective customers, verifying such documents with the original ones/authentic websites and periodical review of such activities are of much importance. Customer Due Diligence at the time of opening of accounts and thereafter at periodic intervals is crucial to minimize operational

*Senior Manager (Retired), Indian Overseas Bank.

risk. Banks have found, by bitter episodes of fraud that the fraudsters had managed to open their accounts by submitting fake/invalid documents. If only the concerned officials had exercised a little care, these frauds could have been averted at the beginning stage itself.

b. *Suspicious transactions and money laundering*: RBI and the Ministry of Finance have been advising banks, time and again, to help the country nab the persons who launder money. Money launderers operate mostly through bank accounts and hence, banks can play an effective role in identifying and preventing such nefarious activities. Fixing threshold limits for customers' monetary transactions in tune with the income levels, monitoring transactions which breach these limits, identifying suspicious transactions which defy common sense and reporting such transactions to the apex office so that they can be escalate to the Financial Intelligence Unit (FIU) of Government of India can be done by the field functionaries. Some KYC-compliant customers act as "money mules" by allowing the operations of their known/unknown clients in their accounts. Branches have the closest contact with the constituents and can monitor their transactions and get the clarifications for transactions which are unusual or abnormal.

c. *Branch upkeep/house-keeping of the service outlets*: Even though it has become common knowledge that Closed Circuit TV (CCTV) can play a vital role both in the prevention of crimes and in the nabbing of criminals, many incidents of daylight dacoits/ robberies have taken place in various banks and regretfully, either CCTV was not installed or it was not functional. This makes the police and investigating authorities grope in the dark, without any vital clues. On the other hand, many such crimes have been solved and money recovered with the help of CCTV footages wherever they were made available.

In an incident involving a branch of a nationalized bank where dacoits had, in broad day light, decamped with a huge cash haul after threatening the staff at gun-point, it was found that there was no CCTV at the branch; luckily, another nearby bank branch had installed CCTV. The dacoits were identified with the CCTV clippings, because they had earlier made a reconnaissance at that bank branch. This helped the police to identify and nab the criminals.

Each Bank should have a policy or frame appropriate guidelines on the necessity of visits to the branch by branch staff on days of continuous holidays. These visits by the branch officials can be on rotation, preferably twice a day. Such guidelines and visits by branch officials will help in checking that no untoward incidents have taken place/attempted. The strength of the grill/wooden windows and possible entry into the strong room/locker room through the back side of the premises should be periodically checked by the branch staff and necessary corrective steps should be taken by reporting rectifications to their controlling offices.

At many bank branches, the house-keeping is very poor. Files and papers are kept/dumped near electrical points. There is water logging and dirt in the UPS room; the UPS room does not have ventilation and high temperature is generated inside the room. If branches/service outlets take effective steps, such situations can be avoided and possible fire incidents can be prevented.

d. *Customer service and operational risk management:* In many banks, signatures of the customers are not scanned at the time of opening of accounts. This results in return of

cheques at the Clearing Houses and the banks are embarrassed when the customer points out to the lapse that though funds were available in the account, cheque had been returned. Undelivered debit/credit cards, PIN mailers, cheque books can pose serious threats to the satisfactory customer service. Many frauds have taken place in the past in these areas. Moreover, deficiency in customer service, can lead to customer escalating his grievance to Banking Ombudsman and consumer court, seeking compensation. This is a big operational risk.

Attending to customers and disposing them in optimum time, not only results in customer delight and mitigation of customer complaints, but will also ensure that potential fraudsters are on guard. Fraudsters find it easy to decamp with cash and other valuables, when the premises are crowded.

Even a polite question "May I help you?" posed to an intruder will put him in check. In a robbery involving a bank branch, a robber had come to the branch and walked into various desks and places within the premises including accessing the cash room and locker room and peeping into the cashier's cabin without any body, not even one employee, asking him what he wanted. Ultimately, he entered the cash cabin and decamped with a huge cash haul.

e. *Disaster recovery and business continuity plan (DR & BCP)*: Branch staff should know the escalation points in case of any disaster-like situation. They should know whom to contact in case of system failure, log-in failure and connectivity issues. They should be aware of the contact numbers/contact personnel /vendors in regard to telephone, fire, police, printer, locker issues. Customers cannot afford to wait for a long time for service to resume and therefore, branch staff should rise to the occasion and ensure Business Continuity with minimum inconvenience to their customers.

f. *Digital banking and operational risk management*: Digital banking has taken the country by storm. Banks have felt the most powerful impact on this. There is no doubt that customer service has improved with the advent of digital products and services but digital banking comes with a lot of operational risks, which banks have to manage. The employees at the grass-roots level-branches and service outlets, should educate their customers on the precautions to be taken in handling digital products and services such as ATM cards and e-commerce transactions through debit and credit cards, internet banking and mobile banking. The staff should advise the customers that their log-in id, password, bank account details should never be shared with any one even when purportedly asked by bank officials.

Conclusion

As we discussed earlier, many of the risks associated with banking operations are addressed and mitigated at the apex level-Central Office or Head Office as they are called. But operational risk is an area where all employees – Branch Head, officers and other staff can play an effective role. If individual branches, from wherever they function-rural, urban or metropolitan sector- work as a team and take conscious steps in identifying, monitoring and mitigating the Operational Risks, they will contribute to their banks' total risk management, since operational risk happens only in the field-level and awareness of branch staff will prevent legal risks, customer complaints, fraud, pilferage, theft. Such an awareness will help in disaster recovery and business continuity.