Abstract

This decade has witnessed an explosion in computing and communication capabilities. These technological advances will continue even with greater speed to increase our ability to acquire, store, process and network the data. As a result, more and more information is being (and will get) shared in day-to-day functions of the banks, making Information Technology (IT) the very lifeblood of banking. And, the issues of security, audit and control can never be overlooked.

In view of the need felt to review the internal controls, inspection and audit system in banks in India, the RBI had constituted a Working Group (in 1995) under the then Chairmanship of Shri Rashid Jilani, the then Chairman and M.D., Punjab National Bank. And, one of the focus areas of this committee was Computer Audit.

The Committee on Banking Sector Reforms (Narasimham Committee – II, 1997) has in the Report dealt with, in detail, the issues in technology upgradation, and observed that most of the technologies that could be considered suitable for India have been introduced in some form or the other as a pilot. The desired success has not, however, been achieved. The committee also dealt with the systems and procedures in the computerised environment and re-emphasised the importance of effective computer-audit procedures in the Indian banking industry.

In 1999, the Reserve Bank of India had published a report of a Committee appointed to examine various issues pertaining to technology upgradation in the banking and financial sector, and to suggest steps for time-bound implementation schedule of Narasimham (II) Committee’s recommendations. This committee (i.e. Dr. Vasudevan Committee) also felt the need for strengthening the IT-audit and security procedures in the banks in India.

In the report (1999) of the Study Group on Large Value Bank Frauds, appointed by the RBI, the study-group has rightly recommended that the banks should evaluate the risks inherent in computerised and telecommunications banking, and place adequate control mechanism for these risks.

Thus, the objectives of this research-study were:

- To identify the gaps in the literature relating to computer audit with reference to
computerised banks in India.

➢ To study the working of the selected bank-branches in computerised environment from the point of view of computer-audit, detection and prevention of frauds/irregularities etc., through computer-fraud risk assessment exercise.

➢ To collect the cases on computer-security breakdowns and computer frauds, for creating awareness among the top management.

➢ To workout and suggest appropriate strategies for conducting computer-audit, and

➢ Finally, offer suggestions on improving deficiencies in computer security and audit-related areas in banks in India.

Keeping these objectives in mind, the following methodology was adopted for conducting this study. Firstly, the review of literature available on IT-audit and other related areas was done. This review helped in identifying the gaps in the literature and scope for further research. In order to assess the present status of IT and IT-audit in banks in India, several visits were made to the Reserve Bank of India (Mumbai), IBA (Mumbai) and several banks of different category. For study purposes, some banks from Nationalised sector, Co-operative sector and Private-sector category were selected. Two Foreign banks in India were also considered during this study. Selecting the banks of each category (i.e. from each sector) helped in understanding industry-level overall situation of IT and IT-audit, and arriving at the overall computer-fraud risk-assessment level of the banks in India. Further, as the level of technology adoption and stake is considerably more in urban and metro areas, the sample of selected branches of each bank is such that most of the branches (of different banks of different types) covered during this study are from urban and metro areas. In case of, for example say Bank NSB1, there is no considerable difference in the level of technology-adoption among these areas. Therefore, it is not attempted to further classify area-wise, the branches covered.

There is a lot of heterogeneity at IT-level (i.e. at hardware-level, OS-level, Software-Development Tool used etc.) among most of the Indian banks. Also, there are at least 2 to 3 TBA/PBA (Total Branch Automation/Partial Branch Automation) –solution-providers in almost all of these banks. Therefore, due precaution was taken to ensure that the sample contains at least one branch having different vendor and different Branch-Automation solution, either TBA or PBA. As the size of a bank is determined here by the number of branches, in case of large-size banks (among Nationalised sector), the number of branches considered is therefore much more than in case of other types of banks. In all, 131 branches/offices of 11 different banks of various categories were selected for this study.

Apart from this, the researcher had interacted with about 1000 techno-bankers and some IT-
auditors during past four years while delivering hundreds of lectures on IT-Audit related
different topics, at NIBM and other national-level institutes. This interaction helped the
researcher a lot in getting the insight of the issues related to this area and its status in different
kinds of banks in India. The researcher also had an opportunity to participate in the
“International Workshop on Security and Audit issues in Client/Server Architecture-based
Systems”, organised by MIS Institute (UK), at Cobham-Surray near London, during
December 1996. Also, a series of discussions were held with the USA-based well-known IT-
Audit consultant Mr. A F Kuong, who was invited at NIBM (in 1996) for conducting two
weeks “Intensive EDP Audit” training programme for IT-auditors from various banks in
India. The researcher had participated in this programme which enabled him in understanding
the trends in this area, and practices followed in advanced countries.

In addition to that, several visits were made to the Switch Centre of the Shared Payment
Network System (SPNS, named as Swadhan) situated at Dadar (Mumbai), and some ATMs
under this network in Mumbai. This was carried out to study the Swadhan ATM-Network,
from security and audit angles.

In order to get better idea about the branch-automation packages being used by the banks in
India, several visits were made to the software-vendors’ site, series of discussions were held
with them (at NIBM), and also the software-audit of their branch-automation packages was
carried out. Wherever the source-code was made available by the software-developer, the
white-box testing of the their product was also carried-out. This helped the researcher get the
insight into the features of these packages, and especially security and audit facilities
incorporated in their packages.

Most of the international audit-firms have now set-up their IT-audit divisions, and have
started offering IT-audit services to the banks and banking-software developers in India. On
behalf of one bank, which is covered in this study, the researcher had an opportunity to study
the IT-audit practices being followed by two of the international IT-audit organisations. The
researcher also got an opportunity to review IT-audit report of one foreign- bank. This IT-
audit was also conducted by an international IT-audit firm.

To assess the present status of IT-audit in banks in India, relevant data was gathered through a
series of discussions with the computer-auditors who had come to NIBM for attending several
training-programmes on this subject. This and other relevant data was also gathered through
a mailed questionnaire. Several visits were made to the selected bank-branches and offices in
Pune and Mumbai, to hold discussions and collect the data related to the business-operations
in IT-environment, and the practices followed for IT-audit.

This study also looked into the organisational and managerial aspects of IT-audit and IT-Security in banks in India to ascertain the deficiencies in the functioning of these areas, and suggested the remedial actions.

Some of the computer-frauds happened at the international level were also referred to during this study. Though computer-frauds might also be happening in the banks in India, most of them are yet to come to the surface or not reported anywhere for various reasons. Based on this methodology, the relevant data was gathered and analysed to do the assessment of computer-frauds risk in banks in India.

The questionnaire was designed as a tool for the assessment of risks in IT-related activities, for the purposes of obtaining signals of occurrence of frauds, and subsequently taking preventive action. The level of fraud-risk was ascertained for the following Risk-Areas (RA):

- Unauthorised use of or access to computer resources,
- Unauthorised release of information,
- Unauthorised copying or use of computer software,
- Unauthorised modification of computer resources,
- Unauthorised destruction of computer resources,
- Unauthorised or malicious denial of access to computer resources, and

For each of these Risk Areas, the Risk Level of that particular area was ascertained, based on the responses. Then, the computer-fraud risk was determined at the branch-level of the bank under consideration. This was repeated for several branches of the same bank, and then the computer-fraud risk was ascertained at the bank level. Same exercise was repeated for other banks (and their branches) of the same type. Again, the same exercise was repeated for other types of banks also. Finally, the computer-fraud risk assessment was ascertained at banking-industry level. The various branches of different banks in the nationalised sector, co-operative sector, private sector and foreign-sector were considered for this study.

Based on the sample chosen it was become possible to give some idea of the computer-fraud risks at the sector-level and at the industry-level. The Nationalised-Sector-Banks are having high-risk (68.28%) of occurrence of computer-frauds. The Co-operative Sector Banks, though having moderate risk (56.79%), it is near to high-level range (i.e. 60-79%). The Private-Sector-Banks are having moderate risk (44.36%) of occurrence of computer-frauds. In case of Foreign Sector Banks, the computer-fraud risk level is moderate (43.53%) which is more or
less similar as that of Private Sector Banks. All the Indian banks together (considered for this study, i.e. excluding foreign banks), though have a moderate risk of 56.48%, it is near to high-level range (i.e. 60-79%).

All the Indian banks (i.e. Nationalised, Co-operative and Private banks) are planning to connect (in near future) their important branches/offices through computer-network. Because of this, these risks can further go up. In view of these risks (and new risks because of induction of new technologies), there is an urgent need to have IT-Audit based IT-Risk Rating and IT-Risk Management systems in banks in India.

Based on the analysis of data collected on the present status of IT and IT-audit in Banks in India, framework for conducting IT-Audit and enforcing IT-security in Banks in India was suggested.

In the area of electronic banking (non Internet-based) in India, we have : EFT and EDI systems initiated by some banks, Off-line and on-line ATMs (Automated Teller Machines, rather, Any Time Money), Shared ATMs (i.e. Shared Payment Network System SPNS called “Swadhan”), and Use of Internet for marketing and preliminary information services. The researcher also studied the functioning of other electronic money-transfer products and services available in the advanced countries. The security, audit & control aspects of these recent developments in Banking Technologies are also discussed in the thesis.

Though we are moving ahead in the deployment of state-of-the-art technology in banks in India, there are many issues related to IT-security and IT-audit of the existing as well as emerging IT in banks in India. It is attempted to discuss those issues, and suggested some remedial actions to resolve these issues. The issues dealt with are related to:

- Information Security,
- Internal Controls,
- Large-scale integrated MIS,
- End User Computing Risks,
- Contingency Planning for Banks,
- IT Risks in Mergers & Acquisitions,
- Network Services and EFT Systems,
- IT Contract Risk and Financial Information on IT-Service Provider,
- Systems Development Life Cycle,
- Evaluation of the purchased/out-sourced software systems, etc.

An attempt is made to give appropriate suggestions to resolve these issues.
The Computer-Fraud Risk Assessment done indicates that there might be frauds occurring in the computerised environment, though most of them are not yet come to the surface, or detected but not reported because of various reasons. This necessitates availability and use of various tools and techniques for strengthening IT-audit related activities and preventing the occurrence of frauds in the computerised environment in banks in India. In fact, there is an urgent need to have industry-wide IT-risk rating and IT-Risk-Management system in existence.

Based on the framework used for collecting data for computer-fraud risk assessment and actual data-analysis based on this framework, a checklist for computer-fraud prevention is suggested. For IT-auditors, this will become a handy tool to use for preventing computer-frauds in their respective banks. The suggested checklist is general in nature, and therefore needs to be modified as per the specific requirements of the banks.

In order to effectively manage IT itself and for managing other IT-related activities like: bank-wide information about various resources, IT-security, IT-audit, contingency planning and disaster recovery procedures, corporate network, branch-level systems administration, RO/ZO/HO -level systems administrations etc., the banks will have to restructure their existing set-ups of IT-Department. So far as the set-up of Audit/Inspection department is concerned, the Jilani Committee had recommended the set-up of IT-audit cell under Audit department, and in almost all the banks it is already in existence. In this context, the appropriate organizational set-up for IT-Security & Audit is also suggested. However, perhaps it may require further modifications based on individual banks existing organisational setup, the level of technology-adoption there, and their specific requirements.

At present, there is neither any IT-Risk Rating System nor IT-Risk Management System existing in any of the banks in India. Based on this research study, it is attempted to initiate the development of conceptual framework for such a system. The Computer-Fraud Risk Assessment exercise carried out during this research-study would become an important milestone of reaching towards a comprehensive IT-Risk Management System. By following the evolutionary approach described in the thesis, such a system will emerge which can then be deployed across the Indian banking industry.

The suggested IT-risk rating System for banks in India may be used for rating the banks (and their branches/offices) based on their quality of doing IT-related activities. This will require the banks internal IT-auditors and/or external IT-auditors and also regulatory authorities to
audit various IT-related activities in various banks. These activities include: IT-Audit, IT-
Management, Systems Development and Programming, IT-Operations, Networking, Overall
Controls over Data, and End-User-Computing. It can also cover any other IT-based-services
given to the customers (internal as well as external customers) at various levels (like branch-,
controlling-office-, and Head-Office -level), and also products and services offered by the IT-
vendors to the banks.

That means, this framework can also be used by the governing authorities to audit the quality
of IT-related policies, procedures and controls established by the management of the banks.
Alternatively, such an IT-audit-based IT-risk rating exercise may be conducted annually by
some autonomous institution on behalf of RBI, on an on-going basis. This will not only help
the banks to become more quality conscious but also improve the overall control over their
IT-related activities and in minimising IT-related risks.

Each computerised-office (i.e. branch or any other office) may be assigned a rating based
upon the quality of conducting various IT-related activities. Each of the critical areas
(mentioned above) and activities therein (whichever are applicable there) may be assigned a
separate risk-rating, and then the branch-level, region-level, zone-level, bank-level and then
eventually at industry-level overall IT-risk-rating can be ascertained.

The thinking of industry-wide IT-Risk Management requires further work in respect of how
an IT-audit-based IT-Risk rating approach might be structured. It is well beyond the scope of
this study to develop a detailed design of the system. Nonetheless, the researcher envisages
that the foundation of this architecture would include the following elements:

- A bank’s assessment of the IT-Risks covering at the minimum the aspects mentioned
above, and the measurable risk characteristics associated with these IT-areas,
- A standard system for classifying those exposures, which may be parameterised by
the Governing authorities,
- Relative importance-weight to be assigned to various IT-related and also IT-based
activities,
- A supervisory/regulatory process for validating this approach, including ways of
ensuring that a rating reflects all relevant information on the underlying risk of an
exposure, and that the process by which rating is assigned ensures its integrity, over a
period of time.

It may also be necessary to increase IT-related areas in the architecture of the IT-Risk Rating
System by having further refinements in the system, for the treatment of new kinds of systems like retail and wholesale Electronic Payment Systems (domestic as well as international), other e-banking services, Data Warehouse-based Decision Support Systems etc. There may also be a need for the recognition of more sophisticated forms of analysing IT-risks, both, for a given bank and at the industry-level.

The framework outlined above provides for a progressive, evolutionary approach to the development of IT-Risk Management System in banks in India. This framework will provide an important input for banks to further improve their IT-Management practices in general and IT-Risk Management practices in particular.

Also, a suitable software system may be developed to automate the data capture and analysis activities of this exercise. Then, such an analysis may be carried out at RCC-level, ZCC-level, at HO-level, and finally at the industry-level. The industry-level analysis and further rating exercise may be carried-out by the apex-level institute like NIBM, on behalf of RBI.

Furthermore, there should be a Task Force/Study Group to monitor the industry-wide implementation of the IT-Risk Rating and Risk-Management systems, to review the system periodically, and improve it on a continuous basis. This will help keeping this system in tune with the rapid changes occurring in IT. This may lead to incorporation of new aspects, modification in the existing ones, deletion of out-dated aspects. There may also be a need to make changes in the relative importance-weights to be given to these areas and the subordinate-level sub-activities in those areas.

The researcher has attempted here to give a conceptual framework of this system. The complete design, development and implementation of such a system is an enormous work, which requires more resources in terms of efforts, money, time, and man-power. A series of workshops on this topic need to be arranged at the apex-level banking Institute like NIBM, for IT-Audit Heads, Chiefs of Inspection/Audit, Chiefs of IT, and representatives of the Governing Authorities. This will help in refining and freezing the design of the system. At the end of each workshop/meeting, the updated draft-copy of the system need to be prepared and then be sent to the RBI for consideration and comments for further refinement. This will help in identifying whether important elements of IT-Risk Management have been omitted or are given insufficient attention. Over a period of time, through a series of incremental improvements, the system can be refined which will reflect the enhancements in industry-level IT-management in general and IT-risk management in particular.
The researcher therefore feels that there is an urgent need for the adoption of the concept of:

- IT-Risk Rating System by the banks in India, and especially by the regulatory authorities, and
- the development of such a system along with necessary software-system

at this juncture. So far as the development of effective IT-Risk Management System at the Indian banking industry-level is concerned, we have really a long way to go.

Implementation of and continuous improvements of such IT-Risk Management System would certainly result in having a very sound and structured IT-practices in the banks in India. This will also minimise the occurrence of frauds and disasters, and therefore will improve the IT-health of the Indian Banking Industry.