3.2 KARNATAKA STATE FINANCIAL CORPORATION

INFORMATION TECHNOLOGY AUDIT OF 'ON-LINE SYSTEM'

Highlights

Not negotiating for the lowest rates quoted for individual items while purchasing hardware for implementation of the 'On-line systems' resulted in avoidable extra expenditure of Rs.30.14 lakh.

(Paragraph 3.2.7)

The application packages lacked many in-built controls and validations to safeguard against incorrect data entries and proper process of data making the information generated by the system not reliable in many areas.

(Paragraphs 3.2.8 to 3.2.10)

The Management has not formulated any policy regarding physical and logical security of IT assets including software and existing data. Insufficient security features in respect of access control, passwords and login control rendered the system vulnerable to unauthorised access and data manipulation.

(Paragraphs 3.2.11 and 3.2.12)

The Disaster Recovery and Business Continuity Plan was neither approved by the Board nor uniformly followed. The data backup was not periodically checked to ensure recovery of data.

(Paragraph 3.2.14)

Introduction

3.2.1 Karnataka State Financial Corporation was established in March 1959 under section 3(1) of the State Financial Corporations Act, 1951 with the main objectives of promoting and developing industrial growth in the State of Karnataka by providing financial assistance in the form of term loans, equity participation, equipment leasing, etc. In the recent years, the activities have been mainly confined to term lending, catering to small and medium scale industries. The Corporation, headquartered at Bangalore, with seven Zonal Offices and 30 Branch Offices is headed by a Chairman and the Managing Director nominated by the State Government, who is assisted by two Executive Directors and six General Managers.

The Corporation, which has been using computers since 1983, established an in-house computer centre in 1985 headed by an Assistant General Manager, mainly for development and maintenance of various applications. The Corporation has an 'On-line system' with 11 modules to facilitate its core activities.

Scope of audit

3.2.2 Audit evaluated the IT controls in the 'On-line systems' of the Corporation for the year 2004-05, which was extended to earlier years wherever required.

Audit objectives

3.2.3 The audit objective was to evaluate the effectiveness, reliability and integrity of the 'Loan Management System' module of 'On-line systems' in particular and other modules, in general, at the Head Office of the Corporation in Bangalore.

Audit criteria

3.2.4 Audit criteria considered for assessing the achievement of audit objectives were manual data; electronic data, wherever made available, and manuals for the implementation of computerisation in the Corporation.

Audit methodology

3.2.5 The sample data of the information contained in data tables received from the IT Department of the Corporation in the form of an Export Dump was scrutinised using the generalised audit software – IDEA.

Brief history of on-line system

3.2.6 The objectives spelt out, for taking up the 'On-line systems', among other things, were to bring in improvement in efficiency and effectiveness, make decisions qualitative through accurate and timely information and monitor projects easily. The 'On-line systems' was to upgrade the relatively stale information existing in the 'batch processing systems' that were in use, provide data on a continuous and updated format to clients/in-house users. As per the original proposal before the Board, 'On-line systems' was to be implemented in 1994-96, by establishing a network between the Head Office and all the branches. However, the 'On-line systems' was developed and implemented in phases over a period of five years (1994-1999), comprised of 11 modules viz., Appraisal, Inspection, Disbursement and Monitoring (IDM), Recovery, Loan Accounting, Finance Accounting, Bills Processing, Insurance, Fixed Deposit, Bonds Management, Line of Credit Systems and Lease Accounting. The actual cost of implementation of the project was

Rs.4.51 crore. The proposal of networking, however, remained unfulfilled and the on-line system was made operational independently in all the branches.

Extra expenditure due to improper evaluation of bids

Non-negotiation for lowest rates quoted for individual items while purchasing the hardware resulted in avoidable extra expenditure of Rs.30.14 lakh.

3.2.7 The Board approved (January 1999) the implementation of the on-line computerisation in the Corporation at a cost of Rs.4.10 crore. However, the tenders were invited in December 1998 itself and the quotations were taken only from four vendors[$]. No justification for resorting to limited quotations for such huge procurement, instead of calling for open tenders to avail the benefit of competitive bids, was on record. The Corporation then split the requirement of hardware among all the four parties and placed orders. It was noticed in audit that the Corporation paid different prices for the same items amounting to Rs.30.14 lakh. The Government stated (December 2005) that the orders for individual items on different vendors were not decided because of compatibility of equipments, after sales service and support. The reply is not tenable as the Corporation could have considered the lowest price of each item and asked the parties to match the same. Further, except one firm (WIPRO) other firms were not the manufacturers of items required and none of them manufactured UPS. Under the circumstances, the action of the Corporation in not negotiating for the lowest rates of individual items among the four vendors resulted in avoidable extra expenditure of Rs.30.14 lakh.

Deficiencies in design and development

Inadequate controls/validations in the system rendered it to be of limited use in facilitating the process of loan Appraisal, Inspection, Disbursement, Monitoring and Recovery as detailed below:

Data capture

The application package lacked many in-built controls and validations to safeguard against incorrect data entries and proper process of data making the information generated by the system not reliable in many areas.

3.2.8 It was noticed in audit that essential details of entrepreneurs like bank account number, passport/permanent account number, net worth, etc., were not mandatorily captured under the pre appraisal/technical appraisal menu. Similarly details regarding the various approvals obtained for a project to be financed, bankers' opinion, demand and supply forecast and rates of depreciation were not compulsorily entered. This seriously limited the usefulness of the information generated by the system to facilitate the process of loan appraisal. The Management stated that approvals of various authorities cannot be mandatory as it varies for different loanees and bankers' opinion contains a subjective element and hence cannot be uniform. The reply is not acceptable as some of the approvals to be obtained were common to all and it was against the provisions of the Loan Disbursement Manual of the Corporation to ignore bankers' opinion.

[$] **HCL INFOSYSTEMS Limited, WIPRO Limited, TATA IBM Limited and Compaq Computer Asia (P) Limited.**

Input control and validations

3.2.9 The system lacks input control and input validations as detailed below:

* In the pre-appraisal/technical appraisal menu, data keyed in was accepted by the system, without any validation checks like

  - Sanctioning of loans beyond the maximum prescribed limits;
  - cases of security offered;
  - jurisdiction of the branch sanctioning the loan; and
  - Promoter's contribution below the minimum prescribed for various schemes.

  As regards validating jurisdictions of branches, the reply of the Management that provisions were made to cover all places is not acceptable as against a district specified places outside the districts should be considered for rejection by the system. Similarly, the reply of the Corporation that validation of promoters' contribution was prompted by the system at the time of generating reports cannot be accepted as it could be overruled.

* In the master table of loan accounts, the next principal due date was beyond one year in 112 cases and extended even up to the year 2010. In a few cases, the next interest due date had already lapsed, i.e. it was less than even the current date. The next interest due date could not have elapsed when the next principal due date was beyond one year. The Management stated (August 2005) that the differences related to pre-closed cases. The reply is not acceptable as in such event a trail should be maintained to prevent loss of data integrity.

* In the Oracle table, containing data on Loan-wise/unit-wise rate of interest furnished to Audit, 7,531 records were there and an analysis of the data in the table disclosed that contracted rate of interest as well as penal rate of interest was zero in 24 cases. As rate of interest cannot be zero, 'nil' rate of interest in the above cases disclosed the lack of input validations. The Management replied (August 2005) that these are closed cases. The reply is not acceptable for the reason that the rates of interest should have existed even in such cases.

* Similarly, the table containing the details of sanction of loan furnished to Audit had 2,150 records and in respect of 123 cases, the rate of interest was zero. The Management stated (August 2005) that for rate of interest the data available in the accounts module is used. The reply is not acceptable as this

deficiency in system design makes the rate of interest keyed in as redundant.

* In the Inspection, Disbursement and Monitoring module the system accepted earlier dates for a subsequent inspection and the entire amount sanctioned could be keyed in for disbursement in addition to the amount already released. Moreover, changes to repayment schedule affecting Debt Service Coverage Ratio were to be keyed in, though the same were available in the appraisal stage; loan repayment start date was to be entered in two stages of loan master table and loan repayment schedule table. It was also observed that the system did not support for recording approval of competent authorities for changes to repayment schedules.

Process control

Deviation from business rules

3.2.10 The system did not alert against deviations from the provisions of the Loan Disbursement Manual of the Corporation like non-inspection of the unit within three months of sanction of loan or when the party approached for disbursement, whichever was earlier. Further, the system did not prompt for inspections due subsequent to disbursement, periodical reminders to loanee in respect of undisbursed loan amounts and to call the borrowers for Project Implementation Review Committee (PIRC) meeting on due dates. Similar prompts in case of partially disbursed cases, to speed up the project implementation or call the borrower before PIRC and prompting communication in cases of cancelled/restricted loans by PIRC to borrowers within 10 days was not supported by the system.

General controls

The Management has not formulated any policy regarding physical and logical security of IT assets including software and existing data. Insufficient security features in respect of access control, passwords and login control rendered the system vulnerable to unauthorized access and data manipulation.

Non formulation of IT Policy

3.2.11 Though the Corporation has over the years developed substantial IT applications, it is yet to formulate and document a formal IT policy and a long term / medium term IT strategy incorporating the time frame, key performance indicators and cost-benefit analysis for developing and integrating various systems. No planning / steering committee with clear roles and responsibilities exist to monitor the development of software for each functional area in a systematic manner which led to avoidable losses and non achievement of objectives of the Corporation. The Government stated (December 2005) that an IT Policy would be formulated shortly with the approval of the management.

Access Control mechanism and segregation of duties

3.2.12 It was noticed that there was no access control matrix document prepared and got approved by the Board. No details of class of individual officers / staff who fall into different categories and how many are designated as System Administrators with full access rights were produced to Audit. Similarly, details of number of officers designated as Database Administrators and their tenure were not maintained. Moreover, duties and functions assigned to system administrators and database administrators were also not documented.

A group of officers were operating with a common password in Accounts Appraisal and IDM Modules. Thus, there was no structured implementation of and monitoring of any password policy. In the two branches visited by Audit, there were no clear guidelines from the Head Office with regard to framing of passwords and also change of passwords from time to time.

The Government stated (December 2005) that the above issues would be covered in the IT policy proposed to be formulated.

Inadequate Change Management Controls

3.2.13 It was noticed during audit that program changes were sent to branch offices as version patches on cartridges. In two branches test checked, the branches had not maintained any record to indicate the actual date of receipt of patch from the Head Office, actual date of copying of patch and the person who carried out the exercise. In the absence of a uniform method to be followed it may lead to a risk of loss of data integrity and incompatibility when all offices are networked. The Government stated (December 2005) that suitable action would be taken in case of future changes to programs.

Lack of adequate Disaster Recovery and Business Continuity Plan

The Disaster Recovery and Business Continuity Plan was neither approved by the Board nor uniformly followed. The data backup was not periodically checked to ensure recovery of data.

3.2.14 No policy was formulated and detailed procedure documented for recovery of data, programs and other software in case of disaster. In two test checked branches as well as in the Head office, it was noticed that there were no off-site backups of the data. Fire fighting equipments were not installed in the server room.

It was noticed in audit that there was no formal policy regarding the frequency of taking back up and test checking it for retrieval. In two test checked branches, the backup data were not being checked for retrieval. In another branch, it was noticed that monthly backup was not being taken.

In the absence of a proper system, the business of the Corporation to the extent it is dependent on the electronic data will be very badly affected in the event of any disaster. The Government stated (December 2005) that refinement of existing policies would be made at the time of making proposed IT Policy being submitted to the Board.

Lack of system testing before implementation

3.2.15 Audit enquiry revealed that no proper testing of the system duly documenting the same was done before using the package. An independent pre-implementation testing at various stages of development would have reduced many inaccuracies in design and development, obviating the effort to key in data all over again. Further, no formal post-implementation review of all the modules was carried out and results thereof documented for necessary follow-up action / maintenance. The Government stated (December 2005) that programs will be thoroughly tested and feedback will be obtained.

Performance of the system

3.2.16 Any computerisation effort has to be supplemented by appropriate input, processing and output controls to ensure confidentiality, integrity, and reliability of the data stored and flowing through the IT applications. However, it was noticed that because of deficient control environment the objectives of the computerisation of improving the efficiency and effectiveness of the organisation have not been achieved even after spending Rs.4.51 crore over a period of five years. The related observations are given below;

* The time taken for sanction of loans had been the same and had even increased in some cases after the introduction of the package, to which the Management stated (August 2005) that the number of days taken for processing the application cannot be attributed to delay in processing by the on-line package. The reply is not acceptable since time taken to process applications for financial assistance being one of the key factors of efficiency, reduction was expected to be realised by the system making all the relevant information available in a timely and accurate manner.

* One of the main objectives of on-line systems was to overcome limitations of batch processing systems. However, the Key data in different modules were still not being entered even after five years and manual files continued to be maintained.

* Vital data about disbursement of loans, extent of utilisation by the beneficiaries and their recovery from the loanees were not being keyed in into the system. They were, therefore, not available to the management for decision making.

- There were no records in some of the key tables pertaining to many topics like details of changes in first investment clause, details of changes in means of finance during disbursement, details of changes in project cost, and details of release with dues with authority for approval.

- No data was found keyed in regarding existing assets of the loanee and details of performance of loanee units gathered on inspection.

- No data was captured for 'conditions imposed' for disbursement of loans, details regarding requests of the loanee for changes regarding working capital arrangements, security offered, etc.

- The number of records in various tables capturing different details of loanees – ranging between 2 and 9,127, varied with the number of records in the master table of loan accounts, which contained 11,480 records. The huge variation in the number of records indicated that data entry in all tables was not mandatory.

The Management stated (August 2005) that these tables were introduced subsequently hence there were differences. It was further stated that the difference related to cases, which were closed prior to implementation of 'On-line systems'. The reply is not acceptable as data for both tables should not be available, if they pertained to old cases. The Management stated (August 2005) that suitable modifications would be incorporated wherever necessary.

Acknowledgement

Audit acknowledges the co-operation and assistance extended by the staff and the Management of the Corporation and officers of the Government at various stages of conducting the performance review.

Conclusion

Structured efforts at computerisation of IT activities would have enabled the Corporation to have a transparent, efficient and effective system to facilitate all aspects of loan appraisal, disbursement and monitoring. However, due to lack of properly directed efforts the Corporation still has a mix of manual and automated process with key areas still being manual, and thus not free from error or discretion. Moreover, the application packages lacked in-built controls and validations to safeguard against incorrect data entries and proper processing of data with the effect that the information generated by the system was not reliable in many areas. Thus, even after spending money and valuable time, the Corporation has not been able to use IT advantageously to bring in transparency and efficiency. This is a serious short coming in an organisation that disburses over Rs.300 crore annually as loans.

Recommendations

* **The Corporation needs to rework its entire strategy towards computerisation to harness true value of IT in not only enabling business but in improving processes.**

* **Proper input, processing and output controls need to be implemented in the organisation. It needs to fine tune the validations to bring them in line with manuals/circular instructions/lending policies.**

* **It needs to formulate and document an IT policy immediately.**