2.4 IT review on Recovery and Billing System in The Pradeshiya Industrial and Investment Corporation of Uttar Pradesh Limited

Highlights

The Company undertook partial computerisation of the recovery and billing system without formulating an overall and coordinated IT Policy or strategy. General and application controls were not effective, user requirements were not defined or documented and physical and logical controls essential to prevent misuse of the system or unauthorised manipulation of data stored were absent.

(Paragraphs 2.4.6 to 2.4.8 and 2.4.12 to 2.4.15)

The software had design deficiencies of controls that facilitated vital fields like names of guarantors, promoters, repayment schedule etc. remaining blank and disbursements exceeding the sanctioned amount.

(Paragraphs 2.4.9 and 2.4.10)

Large differences existed in the data relating to one time settlement (OTS) cases due to non-integration of Recover 2000 with the stand alone data base used for maintaining OTS details. Every body was allowed to change the data as login and passwords had not been provided to different users.

(Paragraphs 2.4.16 and 2.4.21)

Data was unreliable and did not give adequate assurance to integrity and did not have written authorisations and safeguards against theft, damage, protection of programmes/data files etc. It also did not have disaster recovery and business continuity plans.

(Paragraphs 2.4.23 and 2.4.26)

Introduction

2.4.1 The Pradeshiya Industrial and Investment Corporation of Uttar Pradesh Limited (Company) was incorporated in March 1972 as a wholly owned Government Company with the main objective of promoting and developing industries by providing financial assistance to medium and large scale industries already setup or proposed to be set up in the State.

The main objectives of the Company are (i) to carry on the business of an investment Company for providing finance to new/existing industrial enterprises in the State; (ii) to buy, underwrite, invest, acquire and hold shares, stock, debentures, bonds, obligation and securities by original subscription, participation in syndicates, *etc.*; (iii) to carry on the business of Merchant Banking in all its aspects and to act as managers to issues and offers; and (iv) to provide financial assistance on lease and to carry on the business of providing investment and financial services in all their aspects.

The present activities of the Company are mainly confined to recovery of financial assistance provided to industrial concerns through term loans, short-term loans, working capital term loans, Fully Convertible Debenture (FCD)/Non- Convertible Debenture (NCD) and lease assistance.

As on 30 June 2006, the Management of the Company was vested in a Board of Directors consisting of a part time Chairman, a Managing Director and

seven other Directors. The Managing Director is the executive head of the Company and is assisted by two General Managers (Finance and Technical) and a Company Secretary in managing the day-to-day affairs of the Company at the corporate office and a Senior Regional Manager at its NOIDA regional office.

The Information Technology (IT) wing of the Company is headed by a Senior Manager (Technical), assisted by a Data Base Administrator/Manager (Computer), an Assistant Manager (Hardware and Software) and five other staff.

Scope of audit

2.4.2 The scope of IT audit included a review of planning, implementation and monitoring of the computerisation of the recovery and billing system and an examination of controls in the IT application.

Audit objectives

2.4.3 The IT audit of computerisation of the recovery and billing system of the Company was conducted to assess whether:

- there existed an IT strategy and the software was designed/developed as per a properly understood/analysed URS in line with the long term objectives of the Company;
- the implementation of the system was preceded by systematic planning and an adequate assessment of operational requirements and needs and the Company followed a structured approach for System Development;
- the system documentation is adequate and updated to ensure efficient and continuous operation of the system;
- data generated is complete, reliable and follows the business rules of the Company and the users are able to obtain requisite information in the right form and at the right time;
- the physical and logical access controls are sufficient to guard against unauthorised access and to ensure data security and integrity.

Audit criteria

2.4.4 The following audit criteria were used to ascertain whether the objectives stated above were being achieved:

- Approved IT strategy;
- User Requirement Specifications (URS), System Requirement Specification (SRS), System Design Document (SDD) and other manuals;
- Guidelines issued by the Government and rules and regulations of the Company; and
- Security policy & periodicity of security drills prescribed.

Audit methodology

2.4.5 Evidence was gathered through examination of records for existence of an IT policy/strategy, system design analysis, SDLC, BCP *etc.* The data relating to billing and recoveries available upto June 2006 was analysed using

a computer assisted auditing tool *viz.* IDEA* for examining the completeness, availability and integrity of the data. Besides examining the data, the existence and adequacy of general IT controls in the organisation was also assessed.

Audit findings

System Development & Implementation

The development and implementation stage of software lacked systematic and planned approach as is evident from the following:

Lack of IT strategy & absence of a structured development approach

2.4.6 The Company switched over from manual working to semi computerisation based on HCL's Horizon mini computers in 1985-86. During the last 20 years (up to 2005-06) it incurred an expenditure of Rs.2.10 crore on computerisation of its activities but has not adopted a documented IT strategy for setting up both the long term and short term directives for IT systems with the organisation and means required to be adopted to achieve the stated objectives.

The Management stated (July 2006) that the main activity of the Company, *i.e.* term lending is presently stopped, and will be decided after finalisation of a plan for the Company in the near future. The reply does not explain why the Company failed to develop any IT strategy during the past 20 years of computerization. Regarding other issues, the Company furnished no reply.

An organisation undertaking computerisation should follow a structured approach that divides an information system development project into distinct stages that follow sequentially and contain key decision points and sign-offs. This permits an ordered evaluation of the problem to be solved, an ordered design and development process and an ordered implementation of the solution. During the developmental process of recovery and billing system, the Company did not follow a structured methodology as discussed below:

- The Company awarded (December 1999) the work of development of recovery and billing application software to Prosix at a cost of Rs.1.50 lakh. Before award of work, however, no feasibility study was carried out. As a result, the Company failed to incorporate user requirements specifications (URS) clearly while placing the order and specifications continued to evolve during the entire developmental stage. (Consequently, Prosix charged an additional fee of Rs.0.80 lakh for certain items of work terming the same as 'extra items'). The Company further failed to place a consolidated order on Prosix. After completion of 'RECOVER 2000', the Company placed (April 2001) a further order on the same firm for development of a stand alone software package for computing break up of simple, penal and compound interest components of interest over dues (part of billing and recovery system) at a cost of Rs.0.95 lakh.

The Management stated (July 2006) that since the software was to be developed within a very short time to combat Y2K problem, no feasibility study was carried out and that orders for development of various software

* Interactive Data Extraction and Analysis.

were placed as and when necessity arose. The reply is not tenable, as the Company was aware about Y2K problem well in advance. The placement of work orders in piecemeal also shows an unorganised approach.

- System Requirement Specification was also not prepared. As a result, certain items of work (print file of demand bills for two regions simultaneously and taking backup of data from menu) could not be completed by Prosix since the system software (Oracle version 7.0) available with the Company at that time was not supporting the same.

The Management stated (July 2006) that the said items were not needed. The reply confirms the contention of Audit that the Company failed to specify its needs clearly.

- No document signifying completion of acceptance testing was available on record. On actual use, a number of problems in the software were noticed; some of them are still unresolved.

The Management stated (July 2006) that some of the reports developed by Prosix required data since inception that was not available with the Company. Hence, these reports could not be generated in Oracle. The desired reports are being generated on stand-alone system using Dbase. Reply confirms the contention of Audit.

Development of a non integrated system

2.4.7 Billing activity consists of issuing demand bills to the borrowers financed under various schemes *viz.* Term Loan/Equipment Finance Scheme/Equipment Refinance Scheme/Equipment Credit Scheme, Short Term Loan, Working Capital Term Loan, lease assistance and FCD/NCD. During scrutiny of the IT system of the Company, it was noticed that:

- The Company got billing and recovery application software 'RECOVER 2000' developed using Oracle/Developer 2000. In addition, the Company was using 'in-house' developed software 'Payroll' in 'COBOL' (Payroll, recently developed in Oracle is under implementation testing) and 'tally' for accounting purposes.
- The application software 'RECOVER 2000' deals with the billing of term lending only. There was no software for raising demand bills relating to Lease Assistance Scheme and FCD/NCD and billing of cases under these schemes are being done manually.
- The application software 'Recover 2000' failed to yield desired results due to non-feeding of required data input to generate reports/MIRs.

The Management stated (July 2006) that keeping in view the limited number of cases, recovery and billing activity of Lease Assistance schemes was not computerised. In case of NCD/FCD, no reply was furnished.

Absence of system documentation policies and change control procedures

2.4.8 For ensuring efficient and continuous operation, adequate system documentation policy is necessary. However, a number of deficiencies as detailed below were noticed during audit:

- No documentation policies were in existence in the Company, consequently, no documents relating to development, testing, implementation and review of the 'RECOVER 2000' package was available with the Company.
- Though user manual for RECOVER 2000 was available with the Company, subsequent changes made to the software since its implementation (November 2000) was not incorporated in the said manual.

- The Company neither followed nor devised any formal change control procedures to ensure that the modifications in the programme were authorised, tested to the satisfaction of the users, approved and documented.

The Management stated (July 2006) that since no requirement for change in the system had arisen, no policy in this regard has been made. The reply is not based on facts as frequent changes have been made in the software without following change control procedure.

System Design

Audit noticed design deficiencies in the software as detailed below:

Essential fields lying blank

2.4.9 Some of the fields that were essential for maintaining database were required to be made mandatory in the software. In large number of cases, credit of cheques totaling Rs.4,72,36,065.84 has been given to the loanee's account without filling up the necessary information indicating Y (yes) or N (No) in the column depicting bounced cheques. Due to non-provision of mandatory fields, these essential fields were lying blank.

The Management stated (July 2006) that these are either repaid cases or cases that are not in use in the system. The reply is not acceptable as no relevant records were furnished to Audit.

More cases of blank mandatory fields remaining blank have been discussed in paragraph 2.4.12.

Lack of validation checks

2.4.10 Various fields of the software were found to be lacking proper validation as discussed below:

- There was no validation check for rejecting invalid dates. While analysing the table containing details of receipts from borrowers, it was found that in five cases, the software had accepted invalid dates.
- Similarly, while analysing the table containing master data in respect of applications received, it was found that in nine cases software accepted invalid dates in the field 'Sanction date'
- Further, due to absence of validation checks, cases like excess credits given to borrowers account prior to the date of deposits of the cheque, excess disbursement against sanctioned amount, *etc.* discussed in subsequent paragraph 2.4.12 could not be detected by the application software.

The Management stated (July 2006) that the dates have since been rectified. In case of excess disbursement/excess credits, the Management has furnished no reply.

Business rule regarding charging of interest rate not incorporated in the software

2.4.11 Billing through application software was being done in case of term lending (STL/TL/WCTL/EFS/ECS/ERS) only. The Revenue Auditor (RA) in its reports for the quarter ending April 2002, July 2002, September 2002 and January 2003 pointed out that the old (prior to implementation of 'RECOVER 2000') software package of billing prevalent in the recovery cell up to the quarter ending July 1999 was not having the provision of charging two interest rates on overdue interest. Hence, only single rate of interest, that too at the lower one of the two document rates applicable, was being charged on

overdue interest (after implementation of the new software package of billing effective from the quarter ending 31 December 1999, the system of charging of two interest rates on overdue interest as per document rates was started). The RA cited many such cases and to facilitate the Management, it calculated loss of revenue in case of 'VP Rolling and Siddhartha Spinfab Ltd.' for the period November 1999 to January 2003 amounting to Rs.17.05 lakh and also suspected loss of revenue of crores of rupees in the several other cases. The Company, however, recalculated interest (February 2004) in the case of 'Siddhartha Spinfab' and against the overdue amount of Rs.5.26 crore (calculated by old software) corrected the actual overdue to Rs.5.82 crore. A sum of Rs.56.49 lakh was undercharged. The other case files were not put up to audit for review.

The Management stated (July 2006) that the case cited by RA has been recast. However, the case file was not submitted to Audit for review.

Application Controls

Input control

2.4.12 Input controls provide assurance about data integrity. Scrutiny of records and data tables of recovery and billing software 'RECOVER 2000', however, revealed that there was lack of input control as detailed below:

- 48 cases of loan amounting to Rs.93.93 crore were not having the names of any guarantor and the necessary fields in the table were lying blank.
- Similarly, 139 cases of loan were not having the names of the promoters and the concerned fields were lying blank.

The Management stated (July 2006) that in the new application software, the data was ported from Horizon and, therefore, some of the data relating to old/repaid cases might not have been completed at the time of initial stage of computerisation. The reply of the Management is not acceptable as substantial invalid data was found at the time of porting exercise and it was agreed with Prosix that Billing Section would correct/complete the data.

- 11 cases were showing excess disbursements made against the sanctioned amount ranging between Rs.0.01 and Rs.56.00 lakh aggregating to Rs.1.18 crore.

The Management stated (July 2006) that these cases pertain to foreign currency loan released through IDBI and in turn, repayment was made to IDBI by PICUP in Indian currency. As the repayments made to IDBI were of much higher amount as compared to the rupee value of foreign currency released at the time of disbursement (due to devaluation of foreign currency) the disbursed amount was also got altered manually in the records to match the outstanding loan. Other discrepancies were due to distortion of data during the porting exercise from Unix to Oracle (five cases), feeding errors (two cases) and due to rounding off of rupees in lakh (one case).

- Out of 2145 cases of loan disbursed by the Company, repayment schedule in 362 cases (total disbursed amount Rs.70.79 crore) was not available in the system.

No reply was furnished by the Management.

- In 15 cases, amounts credited to loanee's accounts were higher than the amount deposited ranging between Rs.0.23 lakh to Rs.4.43 crore. The total excess deposit, worked out to Rs.5.82 crore.

- In 23 cases, credits of cheques received from the borrowers totaling Rs.1.29 crore have been given to their respective accounts prior to the dates of their deposit ranging between 1 day to 2,955 days (in one of these cases, date of credit was not mentioned).

The Management stated (July 2006) that the table 'amount deposited' was not relevant in Oracle. Regarding credits given to borrowers' accounts with retrospective effect, the Management stated that the dates of deposit have been modified in the database. However, no impact on outstandings against borrowers were shown to Audit.

Process controls

2.4.13 Controls over the manual and automated processes which generate the output using the input data is essential to generate relevant and reliable information. Audit observed deficiencies which are detailed below:

Lack of control on manual ledger/records

2.4.14 As per existing practice, the computer bills are posted in the manual ledger and after recording the receipts during the month/quarter, the balance overdue amount of interest is worked out. The said balance is fed in the computer manually. Thus, the entire billing is based on manual ledger.

- In few cases (Sunil Solvex India Ltd., Linak Microelectronics Ltd. - billing quarter: April and July 2002), it was found that the amount of interest posted in the manual ledger was short. Accordingly, the system generated incorrect/short amount of interest for the subsequent month also.
- Scrutiny of records further revealed that ledger and ledger histories maintained in 'RECOVER 2000' were not updated on regular basis. It was found that latest entries in the ledger history of cases settled under OTS during 2005-06 pertain to March 2003. Similarly, bills are being prepared and cases are being settled under OTS on the basis of manual calculations since ledgers of number of cases settled under OTS were not found updated up to the completed quarter prior to the month of OTS.

The Management stated (July 2006) that the short posted amount of interest had since been rectified. No reply regarding updation of ledger and ledger histories was furnished to audit.

Incorrect calculation of interest on loans

2.4.15 As per guidelines issued by the Company, recovery from a loanee is adjusted against its dues starting from the loan having lowest rate of interest (The interest is further subdivided into simple, penal and compound proportionately) and moving towards higher rate of interest. Test check in audit revealed six cases in which the output derived, deviated from the desired results as narrated below:

- Scrutiny of records revealed that in certain cases, the priorities of bifurcation, as fixed by the Management, were not adhered to. In case of other loans (other than working capital term loan) of few borrowers (Kanpur Strips: July 2002, Eggro Fibres: April 2002, Coir Cushions, Charu Papers: January 2003)), it was noticed that instead of making adjustment against loan having the lower rate of interest, the Company adjusted the same against loan having higher rate of interest causing revenue loss to the Company.

- In large number of cases, two different rates of interest have been sanctioned by the Company in case of same loan account (especially in case of additional loan *etc.*). Thus, there were two or more documented rates of interest in the same loan account. In audit of revenue leakage, it was noticed that in two cases (Om Beverages and Elite Appliances: Billing Quarter April 2002 and July 2002) rate of interest lower than the approved/documented rate was charged from the borrowers. This resulted in revenue loss of Rs.3.69 lakh.

- As per the business rules of the organisation, the closing balance of outstanding loan against each borrower appearing in the ledger should be calculated as opening balance (+) debit transaction (–) credit transaction. However, a review of the ledger table in the system revealed that out of a total number of 44,274 records, in 5953 cases this formula was not followed. In 1982 cases, the closing balance shown as per the ledger was more by Rs.1059.29 crore than as per the formula computed value and in 3971 cases, the computed amount was more than the ledger balance (Rs.951.93 crore). This discrepancy needs to be investigated to rule out any unauthorised modifications to the database.

In case of adjustment of receipts contrary to the priorities fixed by the Company and charging of lower rate of interest, the Management stated that irregularities have since been rectified. Regarding difference in Opening and Closing Balance without any transaction, no reply was furnished by the Management.

Inconsistencies in data relating to One Time Settlement (OTS) cases

2.4.16 In order to improve recoveries from chronic defaulters who obtain stay orders from the Hon'ble High Court against notice issued under Section 29 of SFC Act, 1951 and also to reduce Non-Performing Assets (NPA), the Company allows OTS of the outstanding dues as per guidelines of the scheme applicable from time to time. The amount of OTS is normally recovered in one installment or within 12-18 months in monthly/quarterly/half yearly installments.

It was observed that though the option for maintaining OTS details was available in the application software 'Recover 2000', the same was not being used by the Billing Section. The details were being maintained in a stand-alone database on d-base. This has resulted in development of a non-integrated system of application software.

Since the details relating to OTS is being maintained in a stand alone software, there was mismatch between OTS details as per data of 'Recover 2000' and the data available in the stand alone software as detailed below:

(Rupees in lakh)

Sl. No.	Month of OTS	Name of the Company	Amount outstanding as per OTS statement on d-base		Amount outstanding as per ledger maintained in 'Recover 2000'		Remarks
			Principal	Interest	Principal	Interest	
1.	March 2006	Gupta Paper Mills	82.75	74.04	82.75	2213.86	Heavy difference of Rs.2179.82 lakh in interest
2.	Dec. 2005	Orphic Resorts Ltd.	595.24	1945.21	595.24	1813.24	No entries in the electronic ledger after record date 31.07.05. Difference of interest Rs.131.97 lakh
3.	May 2005	Perfect Latex	104.18	702.40	104.18	670.91	No entry in the electronic ledger after record date 31.1.05. difference of interest Rs.31.49

(Rupees in lakh)

Sl. No.	Month of OTS	Name of the Company	Amount outstanding as per OTS statement on d-base		Amount outstanding as per ledger maintained in 'Recover 2000'		Remarks
			Principal	Interest	Principal	Interest	
4.	May 2005	Propene Products	35.69	54.86	35.69	50.65	No entry in the electronic ledger after record date 31.1.05. difference Rs.4 lakh
5.	Sept. 2005	Pacquick Industries Ltd.	165.50	214.75	197.12	214.75	Difference of Rs.31.62 lakh
6.	Dec. 2005	Vee Aar Polymers	75.58	667.77	75.58	787.31	Difference of Rs.19.24 lakh

The case-wise replies furnished by the Management were as under:

Gupta Paper Mills:

- All the dues, except principal and interest amounting to Rs.28.75 lakh and Rs.74.04 respectively, have been written off;

Orphic Resorts Ltd. & Perfect Latex:

- The OTS has been finalised on the basis of manual ledger. The ledger maintained in the application software will be updated accordingly;

Propene Products:

- Rs.4 lakh received in October 2000 adjusted against interest dues was subsequently adjusted against principal dues of the Company as per decision of the settlement committee;

Pacquick Industries Ltd.

- Earlier, simple interest of Rs.31.62 lakh was funded but at the request of the borrower, the case was settled under OTS by nullifying the funding and recalculating the simple interest from the beginning;

Vee Aar Polymers

- After settlement of case under OTS, the borrower again approached the Company for reconsideration of its payments made during 1996-97 against dues of current OTS. Accordingly, the account of the borrower was recasted by deleting earlier recoveries for adjustment of the same against current OTS. This inflated the current dues of the borrower. The Board, however, did not approve the said recasting.

The replies in themselves are ample indicators of actual state of affairs in settlement of dues under OTS.

- It was also observed that despite finalisation of OTS in certain cases (*viz.*, G.S. Rubbers Limited, Nutech Packagings Limited, Vee Aar Polymers Limited–OTS finalised in March 2006, December 2005 and December 2005 respectively), the billing was continuing. Incidentally, all the three borrowers have been shown as regular in paying their dues.

The Management stated (July 2006) that billing in case of G.S. Rubber Limited is continuing since the OTS was not approved by the Settlement Committee. In respect of other cases no reply was furnished.

Use of System as a tool for MIS

2.4.17 Audit found that data available in the System was not effectively used

as input for MIS. Details are given below:

Non-maintenance of data-base relating to relief allowed to assisted units

2.4.18 As per policy of the Company, some relief is provided to the borrowers by deferring the principal or/and funding the interest. Further, the Company also allows reschedulement of loan and gives other concessions and relief under its rehabilitation scheme to the borrowers facing problems in repayment of their dues.

- Scrutiny of data maintained in 'Recover 2000', however revealed that the Company did not have any data-base relating to cases of reschedulement of principal.
- 'Recover 2000' has the provision of generating statement showing deferred/written off principal and funding/ waiver/write off/abandonment of interest for the last 2 years (MIR 7) but monthly information report was not available on the system.

No reply was furnished by the Management.

Non-availability of data-base relating to recovery proceedings

2.4.19 For clearance of defaults, the Company issues follow up letters and arranges meeting with the borrower. In case of failure, the Company issues Demand Show Cause Notices (DSCN) to the borrower/guarantor and thereafter issues Recovery Certificate/notice under Section 29 of SFC Act, 1951 demanding therein payment of dues within a specific period. In case of non-adherence, next step for attachment of the financed unit and deployment of security guards is taken. Thereafter proceeding for sale is started. The amount realised on sale is first adjusted against the principal and then against the interest dues.

It was, however, noticed that:

- Recovery proceedings, like DSCN, notice under Section 29 of S.F.C. Act, 1951 and Recovery Certificates issued by the Company was not made integral part of the application software to have a direct, clear and transparent status of any loan. No provision was made in the software to produce these details.
- Similarly, no database relating to units attached/expenditure incurred on deployment of security guards and units sold alongwith realisation made *etc*. adjusted against various dues and balance recoverable amount. is available in the application software.

No reply was furnished by the Management.

General Controls

2.4.20 The controls which govern the environment in which IT operations are run, called as General Controls, are vital to ensure confidentiality, integrity and reliability of the information processed and stored in the system. Audit observed a number of deficiencies which are detailed below:

Absence of user privileges and data security

2.4.21 Prosix Softron (P) Ltd., vide its letter dated 2 September 2000, observed that the data security in Recovery and Billing system was not proper as everybody was allowed to change the data in the main ledger and further added that changes in the record made by an officer without knowledge of the

concerned officer has caused inconsistency in the data and suggested identification of officers who can select, insert and modify the data and to provide separate log in and password to these users.

However, the problem is still persisting in the Billing Section as no separate login and password has been provided to different users and one Assistant Manager of the Billing Section, looking after the billing of one region can select, insert and modify the data of other Assistant Manager (looking after other region) also.

The Management stated (July 2006) that only officers of Billing Section have the right to access the database. The reply does not address the point raised by Audit.

2.4.22 Scrutiny of recovery and billing proceedings on 'RECOVER 2000' revealed that there was no output control. Select/Add/Modify facility was not only available to all the end users of Billing section but it was also available to the system installed in computer section without any access control. Availability of add/modify facility to all the officers/staff of billing/computer section with non- frozen data, shows lack of control as the bills/ledgers/reports with any kind of modifications can be generated without leaving trace of modifications in the absence of any audit trail.

The Management stated (July 2006) that Add/Modify facility is available to the team of Billing section only without which the section cannot run smoothly. Reply is evasive as the online facility of the same is available in the computer section also. Further, integrity of data cannot be ensured in the absence of any kind of out put control.

Unreliable database due to deficient change management process

2.4.23 The Study conducted by Audit revealed that the system does not give reasonable assurance for integrity of data that is evident from the following facts:

- The software does not freeze any data. Any kind of changes can be made in any data table on any subsequent date;
- The source code is not protected. Some cases of changes made in the logic of the software, are discussed in paragraph 2.4.15 *supra*.
- With non-frozen data tables and add/modify facility available to every end users, any type of bills/ledgers/reports can be generated with suitable modifications as has been discussed in paragraph 2.4.24 *infra*.

2.4.24 During review of General Controls it was noticed that:

- In the Computer Centre, no records relating to written approvals for providing access to the staff were available.
- In Billing Section, general authorisations have been given to the employees without making proper analysis of minimum access requirement to discharge their duties.
- Report and Query rights associated with the module were provided generally to all the users working in the Billing Section, without making analysis of need to know/need to work.
- The Company had not assessed the exact requirement of software

licenses and had not procured the required software wherever necessary.

The Management stated (July 2006) that (i) since the Computer center is service and support department, written approvals for providing access to its staff is not needed; (ii) only team officers are authorised to have access to the billing software;(iii) since they are the officers of billing section, they have all the rights to generate any report and queries relating to recovery and billing; and (iv) valid software licenses will be purchased on restart of the activities of the Company.

The reply is not tenable as these controls are necessary for reliability of data.

Deficiencies in physical and logical access controls

2.4.25 Physical access controls aim at safeguarding the computer equipment from unauthorised access, theft and damage due to accidents/deliberate actions *etc.* while logical access controls protect the programmes and data files from unauthorised access, modification, copying and deletion. Such access controls were absent in the computer systems implemented by the Company. It was also observed that:

- the Company lacked a formal IT security policy and no security drills had either been framed or conducted. Access to computer rooms was not regulated or restricted. Physical security of the main server has not been ensured since it was easily accessible to visitors and staff of other departments;

- firewall to protect the system from outside access through internet was not available

- the Company lacked a well-defined and documented password policy. Passwords were not being changed periodically. Though features of user-id and password were available in the software, the safeguards were inadequate as (i) the date and time of last access and number of unsuccessful attempts after last successful login attempt were not displayed on the screens of authorised users at the time of login; (ii) there was no validation check to reject creation of password of very short length (iii) alpha-numeric passwords were not enforced by the system; (iv) passwords were not case sensitive; and (v) both the user-id and password were the same.

No reply was furnished to audit.

Lack of adequate disaster recovery and business continuity planning

2.4.26 The Company did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that the data processing operations could be regained effectively and in a timely manner, should a disaster render the automated systems non-operational. The key configuration items (hardware, software, personnel and data assets), which were indispensable for continuity of the IT activities had not been identified through a proper risk analysis and counter measures were not outlined.

It was further observed that:

- The fire fighting equipment installed in the corporate office during the year 1991 at a cost of Rs.40.90 lakh that covers the Computer Section also (where main server is also installed) was not in operation (June

2006).

- Fireproof almirah for keeping the back up and other electronic devices was not available with the Computer Section.
- Log of daily/weekly back ups being taken by the Computer Section are not being maintained.

In the absence of a 'business continuity and disaster recovery plan', a significant disaster impacting the Company's servers and other computing systems runs the risk of paralyzing the computerised system of the Company that would seriously hamper its recovery efforts.

The Management stated (July 2006) that all the precautions like taking backup and keeping the same in separate almirah as well as dissimulation of data in three hard disks, are being taken. Further purchase of firewall is under consideration. The reply is not tenable as the measures being taken are insufficient.

Discrepancies in hardware and software inventory controls

2.4.27 Audit scrutiny revealed that the IT wing of the Company did not maintain any record of its IT related inventories. The entries in the registers of the stores section of the Company did not indicate name/type of hardware, its cost, source of purchase, invoice details along with dates. The current stock register shows 'Computer/PC-AT/484 System/PC XT/Pentium: 146 Nos' 'Printer: 100 Nos.' Entries relating to software purchased from time to time could not be traced in the stock registers. There was no evidence that annual physical verification of inventory has ever been carried out, or that items listed in the stock register were being periodically reconciled to the physical inventory.

No reply was furnished by the Management.

Acknowledgement

2.4.28 Audit acknowledges the co-operation and assistance extended by different levels of officers of the Company/Government at various stages of conducting the performance audit.

The above findings were reported to the Government in October 2006; the reply is awaited (October 2006).

Conclusion

The Company undertook computerisation of its activities without formulating an overall and coordinated IT Policy or strategy. General and application controls were not effective, user requirements were not defined or documented and physical and logical controls, essential to prevent misuse of the system or unauthorised manipulation of data stored, were absent. The software designed for recovery and billing of dues 'Recover 2000' is not being utilised in full and lacked effective validation checks, which resulted in revenue loss to the Company.

Recommendations

- **The Company should formulate a coherent IT strategy defining *inter-alia* the goals and objectives of the intended computerisation and benefits that would accrue from it. It is essential that an integrated software package be developed which can take care of the entire business operation of the Company especially functional**

areas of recovery and billing.

- **The Company should ensure documentation of all stages of the system development and the changes carried out to the system at a later date to ensure its smooth and error free functioning.**
- **The Company should ensure adequate physical and logical access controls so that the safety and security of data is not compromised. Besides, adequate input controls including validation checks should be embedded in the software to avoid data manipulation or erroneous data entry.**