CHAPTER 2
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

DEPARTMENT OF POSTS

Information Technology (IT) Audit of Sanchay Post Software

HIGHLIGHTS

* **DoP introduced Sanchay Post software in post offices for computerisation of Savings Bank operations. However, even after seven years of its introduction, operations were computerized in only five *per cent* of the post offices.**

(Paragraph 2.10.1)

* **Sample checks revealed that insufficient validation controls and inadequate monitoring resulted in minus balances in individual savings bank accounts to the tune of Rs 12.26 crore.**

(Paragraph 2.7.2.10)

* **Sample checks also revealed that the software permitted deposits amounting to Rs 7.14 crore under the Monthly Income scheme and Rs 5.08 crore under the Public Provident Fund scheme in excess of the prescribed maximum limits. Interest amounting to Rs 39.35 lakh was allowed on such irregular deposits under the Public Provident Fund scheme.**

(Paragraph2.7.2.8 and 2.7.2.9)

* **The software did not calculate service charges amounting to Rs 6.51 lakh in respect of silent accounts.**

(Paragraph 2.7.2.12)

* **DoP did not pay adequate attention to the various stages of system development such as user requirement specification, testing and implementation. As a result, the deficiencies in the software could not be removed at the development stage itself.**

(Paragraph 2.8)

* **Neither the IT security controls were adequate nor DoP had a business continuity and disaster recovery plan which put the business operations to the risk of system failure and disruption of services.**

(Paragraph 2.9)

- **DoP did not have a proper change management procedure in place, resulting in non-incorporation of new schemes and changes in business rules.**

(Paragraph 2.10.2)

- **The software lacked customer friendly features like automatic transfer of funds from one savings scheme to another, which were available in the software used in banks.**

(Paragraph 2.10.3)

SUMMARY OF RECOMMENDATIONS

- **DoP should implement the software in more post offices in a time bound manner after rectifying the deficiencies mentioned in this report.**

- **DoP should review the package to eliminate areas where controls to ensure data integrity were not adequate and further explore the possibility of introducing a centralized networked banking software.**

- **DoP should ensure that validation controls are in place so that inputs violating departmental rules were not accepted. DoP should re-engineer the software to automatically uninstall the data entry module once the online module was utilized.**

- **DoP should ensure complete incorporation and availability of POSB rules and tax requirements in the software.**

- **Databases should be regularly validated by IT trained internal audit teams on a periodic basis.**

- **DoP should adopt proper change management mechanism to handle changes in software requirements and incorporation of changes in rules.**

- **DoP should have in place strong IT security controls and a business continuity and disaster recovery plan so that system failure and disruption in services do not occur.**

- **DoP should explore inter-connectivity of each post office, and utilize its network of post offices, through adoption of web-based technology, to provide 'any time any where' banking services.**

2.1. INTRODUCTION

The Post Office Savings Bank (POSB) is the oldest and largest banking institution in the country. The Department of Posts (DoP) runs POSB as an

agency on behalf of the Ministry of Finance (MoF), Government of India, which remunerates DoP for this work. The remuneration to DoP for discharging various responsibilities relating to the Savings Bank (SB) increased from Rs 969.87 crore in 1998-1999 to Rs 2,029.82 crore in 2004-2005. POSB offers various savings schemes* through its Head, Sub and Branch post offices (POs) for the convenience of the public.

In order to modernize its services and computerize the entire work of the savings bank branch including activities such as interest calculation, transfer of accounts and closure of accounts, DoP felt the need for a separate software. Accordingly, for Savings Bank (SB) operations in post offices, M/s Datanet Corporation developed the 'Sanchay Post' software on Windows NT platform with Microsoft SQL Server as RDBMS and Power Builder as the front-end tool. The software was upgraded from time to time and the latest version, "Sanchay Post 4.5" was introduced in January 2003. The software handled schemes relating to Savings Bank, Recurring Deposits, Time Deposits, National Savings Certificates, Public Provident Fund Accounts and Monthly Income Account.

The Postal Services Board (Board) is the apex management body of DoP, comprising the Chairman and three members holding functional portfolios of Operations, Development and Personnel. The Deputy Director General (Technology) under Member (Operations) and the Deputy Director General (Financial Services) under Member (Development) look after computerization and SB work, respectively. The country is divided into 22 Postal Circles, each headed by a Principal Chief Postmaster General/ Chief Postmaster General. The work of SB is being carried out by the post offices across the country.

2.2 SCOPE OF AUDIT

The Information Technology (IT) Audit of Sanchay Post was conducted during April to September 2005, covering its implementation and functioning in various General Post Offices(GPOs)/ Head Post Offices(HPOs)/ Sub Offices (SOs). Out of 445 GPOs/HPOs/SOs in all the 22 postal circles where the software had been installed, 116 GPOs/HPOs/SOs in 20 postal circles were randomly selected for audit as detailed in Annexure-I.

2.3. AUDIT OBJECTIVES

The objectives of audit were to examine whether:

- the software functioned efficiently and effectively to carry out the savings bank operations;

* Savings schemes like Savings Bank (SB), Recurring Deposits (RD), Time Deposits (TD), National Savings Certificates (NSC), Kisan Vikas Patras (KVP), Public Provident Fund Accounts (PPF), Monthly Income Account Scheme (MIS), National Savings Schemes (NSS), Senior Citizens Savings Scheme (SCSS), etc.

- system development methodology was in line with the requirements of computerisation;
- security controls associated with the system were adequate; and
- the software adequately addressed the business needs.

2.4 AUDIT CRITERIA

Audit criteria included the following:

- the extent of validation checks in place to ensure completeness and accuracy of data;
- the extent of monitoring to prevent irregular transactions;
- the extent of compliance with the standard business practices of IT system development and implementation;
- the extent of implementation of standard IT security controls, and
- the extent of adequacy of change management mechanism to address the changing business needs.

2.5 AUDIT METHODOLOGY

Audit commenced with an entry conference on 24 June 2005 with DoP where the objectives and methodology of audit were explained. Audit methodology included scrutiny of files and other records at DoP Headquarters, Circle Offices and functioning of the software at selected post offices with the help of Computer Assisted Audit Techniques (CAAT) like Structured Query Language (SQL) queries and use of menu facilities as also interactions with the auditee. This IT Audit was based on the Control Objectives for Information and Related Technology (COBIT), an internationally accepted control standard for IT management and audit. The report was issued to DoP on 8 November 2005 and subsequently a exit conference was held with DoP on 22 December 2005 where the audit findings were discussed. Views of DoP expressed in the conference have been suitably incorporated in the report.

2.6 AUDIT FINDINGS

For efficient and effective functioning of SB operations, it was imperative that the software being used had all the necessary validation controls to ensure that the accounts were opened as per the rules; deposits were accepted only up to the prescribed limits; interest was paid only where due and various other business rules were incorporated. Audit observed that the software lacked adequate validation controls, which resulted in either irregular transactions or unnecessary manual controls. Audit also observed that these deficiencies could be traced to the

flawed system development methodology followed by DoP while developing the software. The IT security controls were not adequate. DoP had not made sufficient efforts to ensure that the software kept pace with the changes in the business needs.

These deficiencies are discussed below.

2.7 LACK OF VALIDATION CONTROLS

Strong validation controls were required at the stage of creation of master data and also during online transactions so that the software accepted only complete and valid inputs and carried out transactions in accordance with the business rules. Audit observed that the Sanchay Post (software) lacked adequate validation controls at both these levels. As a result, the basic risks associated with savings bank operations such as irregular opening of accounts, excess withdrawals, acceptance of deposits beyond permissible limits and payment of undue interests could not be adequately addressed. The risks of fraud and collusion could also not be mitigated. Besides, reliance on manual controls continued.

The inadequate validation controls in the software are discussed below.

2.7.1 Inadequate validation controls in the Data Entry Module

The software had a data entry module separately for each savings scheme which was used for creating master data during the initial stages of computerization at the post offices. Once all data were entered, the data entry module was to be un-installed and transactions had to be carried out through the online module. DoP issued instructions in September 2000 to its field units to complete the entry of historical/old data by the post offices before operating the online module and uninstall the data entry module once the scheme became online.

Audit observed that the data entry module permitted entry of all types of data without any validation to restrict the transactions within the business rules of the particular scheme to which the data pertained.

Further, the software was not designed to automatically disable the data entry module once the software became online and required manual un-installation. Audit observed that DoP's instructions regarding un-installation of data entry module were not followed in a number of cases and both the data entry and online modules functioned simultaneously. This allowed supervisors to access the database laterally and make modifications in the transactions made in the accounts. These manual interventions gave scope for tampering of data.

2.7.2 Inadequate validation controls in the online module

2.7.2.1 Irregular opening of Savings Bank Account

The Post Office Savings Account Rules, 1981 stipulated that a person could open any number of single accounts, but not more than one account at one post office. They also stipulated that a lawfully constituted institution or body could open a public account without any monetary limit for encouragement of thrift or for mutual benefit of its members.

Analysis of the database in 17 HPOs in six circles revealed that 6,656 duplicate accounts were opened in the same name as shown in Annexure-II. The local management accepted the deficiencies.

Audit observed that these deficiencies were due to the fact that whenever a new account was opened by a customer, the software accepted the name, address, etc, and created an account number. The account number so created was the primary key* through which all the transactions of the customer were identified in the database. This indicated that the software did not have the necessary validation controls for ensuring that individuals, using the same name and address, did not open duplicate accounts.

A test check of the database of Indore General Post office under the Madhya Pradesh Circle revealed that M/s Bharati Telenet Limited (BTNL) was allowed to open an institutional SB account for depositing telephone bills by its subscribers in contravention of the rule which permitted such an institution to open a public account only for encouragement of thrift or for mutual benefit of its members. Interest of Rs 0.86 lakh was also allowed.

The local management accepted the audit observation and stated that the account was opened as per orders of the higher authorities and that the interest had since been disallowed. This is indicative of weak internal controls. Audit also observed that the source document, viz., SB-3 form used for opening of an account did not have option for entering complete details of accounts being applied for such as group accounts, institutional accounts, pension accounts, etc as a result of which it was difficult to replicate the same in the database for validation.

2.7.2.2 No provision for storing registration numbers of trusts while opening Time Deposit (TD) accounts

The Post Office Time Deposit Rules, 1981 stipulated that a trust, which was registered under any law, could open a TD account. A non-registered trust could not open a TD account. As such, the complete details of the trust like name

* Primary key is a value that is used to identify a unique row in a table. It is the field in a database table that is indexed and maintains the main sequence of the table.

and registration number should be available in the database in order to ensure that only registered trusts are allowed the facility.

An analysis of the database in one HPO in Rajasthan Circle revealed that four accounts with a total deposit of Rs 3.68 crore were opened in the name of a trust. However, the authenticity of the registration of the trust could not be ascertained, as there was no provision in the relevant table to record registration numbers of these trusts. The local management accepted the fact.

Here again the source document, viz., SB-3 form used for opening of an account did not have the option for entering the registration number of trusts, as a result of which it was difficult to replicate the same in the database for validation.

2.7.2.3 Opening and operating of savings bank accounts by minors

The rules stipulated that a single account could be opened/operated by a minor by himself, if he had attained the age of 10 years, or else through a guardian. Further, joint account could be opened only by two or three adults.

Audit examination revealed that the software permitted opening of accounts on behalf of minors even before they had attained the age of 10 years. Dummy data inputs and subsequent analysis of the database in audit revealed that there were no controls in the software to validate age based on the 'date of birth' field. The software even accepted empty 'date of birth' fields and 'relationship' fields. Also, in cases of opening of joint accounts, it did not restrict opening of accounts by minors along with adults.

The local management accepted the fact and stated that the software was deficient to that extent and the matter was being taken up with DoP to rectify the software.

2.7.2.4 Ineffective controls to check opening of NRI accounts

Non Resident Indians (NRI) were not permitted to open accounts in POSB. The software did not have a provision for identifying opening of accounts by NRIs separately. A check of the source document itself (Form SB-3) used for opening of an account, revealed that there was no provision for identifying applicants' resident status.

The local management accepted the fact and stated that the software needed modification.

2.7.2.5 Opening and operating of savings bank accounts without name

In POSB, a customer is required to fill his name, address, etc in the required form while opening an account. These details are fed into the database and are important for identification of the customer.

Database analysis in the Andheri, Aurangabad and Nagpur Head Post Offices under the Maharashtra Circle revealed that the account holders' names in 188 cases were meaningless alphabets such as X, XX and XXX. This showed that the software accepted even a single alphabet as a customer's name and permitted opening of accounts with such names. This was later confirmed by Audit through entry of dummy data.

On this being pointed out, the Postmasters of the Aurangabad and Nagpur Head Post Offices confirmed the facts and stated that the names of the customers were not available in the ledger and the mistake had occurred at the time of transfer of data from the manual ledgers to the database. Adequate validation controls in the data entry module would have prevented the mistake.

2.7.2.6 Acceptance of deposits in excess of the prescribed limit for single and joint individual savings bank accounts

The Post Office Savings Account Rules, 1981 stipulated that a person could open any number of single individual accounts, but not more than one account at one post office and the maximum balance excluding interest in one account or all the accounts taken together should not exceed Rs 1 lakh. Similarly, two or three persons could open any number of joint individual accounts but not more than one joint account at one post office and the maximum balance, excluding interest in an account or all the accounts taken together, should not exceed Rs 2 lakh.

An analysis of the database in 79 HPOs in 18 circles revealed that in 9,499 instances, deposits were accepted in excess of the prescribed limits as shown in Annexure-III. The local managements accepted the deficiencies and stated that the deposits had been accepted through the data entry module. It was also stated that excess deposits were accepted from the public in the interest of business.

The replies confirmed that the software did not have the necessary validation checks to prevent acceptance of deposits in violation of rules and also showed that the instructions issued by DoP for disabling the data entry module had not been followed.

2.7.2.7 Interest allowed on savings bank accounts having balances above the maximum limit

The Post Office Savings Account Rules, 1981 stipulated that no interest should be allowed on an account on any sum in excess of the maximum permissible limit.

An analysis of the database in 24 HPOs in nine circles, in respect of 187 cases, showed that interest amounting to Rs 21.19 lakh was allowed even in cases where the balance at credit was in excess of the prescribed maximum limit as detailed in Annexure-IV.

The local management accepted the facts.

2.7.2.8 Software permitted opening of multiple public provident fund accounts and irregular transactions

The Public Provident Fund Scheme, 1968, stipulated that only one account could be opened in one name for any amount not less than Rs 500 and not more than Rs 70,000 in a year.

- An analysis of the database in seven HPOs in the Rajasthan and Tamil Nadu circles revealed 32 instances where a customer had opened more than one account.

- An analysis of the database in 39 HPOs in 12 circles revealed that in 1,402 cases, deposits amounting to Rs 5.08 crore were made in excess of the prescribed maximum limit as shown in Annexure-V. In six HPOs in the Rajasthan, Tamil Nadu and Uttar Pradesh circles, interest amounting to Rs 39.35 lakh was allowed on these irregular deposits.

The local management accepted the fact and stated that the above deficiencies arose due to wrong feeding of data. This pointed to the need for effective training and strong validation controls in the software to eliminate their recurrence.

2.7.2.9 Deposits beyond the prescribed limit for single and joint MIS accounts

Rule 4 of the Post Office (Monthly Income Account) Rules 1987 stipulated that a depositor could operate more than one account under these rules subject to the condition that deposits in all the accounts taken together did not exceed Rs 3 lakh in a single account and Rs 6 lakh in a joint account.

Analysis of the database in 47 HPOs in 13 circles revealed that there were 452 accounts with deposits totalling Rs 7.14 crore where deposits were made in excess of the prescribed limits as shown in Annexure-VI.

The management of the Gujarat, Himachal Pradesh and Tamil Nadu circles stated that the accounts were joint accounts and were incorrectly entered as single accounts through the data entry module, while the management of other circles stated that the matter was under investigation. The reply confirmed the fact that the software lacked controls not only to enforce the monetary limits pertaining to single accounts but also to throw out exception reports of these violations.

2.7.2.10 Withdrawals in excess of available credit in savings bank account

A banking software should have necessary inbuilt controls which prevented customers from withdrawing amounts in excess of the balance at credit.

Strong controls should exist for preventing excess withdrawals, as POSB rules did not permit this.

An analysis of the database in 72 HPOs in 13 circles revealed that in 24,264 instances, withdrawals were allowed in excess of the available credits. This resulted in minus balances in individual accounts of the customers amounting to Rs 12.26 crore as shown in Annexure-VII. The Management replied that action was being taken to regularize the same.

The existence of minus balances in a large number of cases showed that the relevant controls in the software were not available and regular monitoring of the database and its records was not being done.

2.7.2.11 Irregular Processing of Recurring Deposits

The Post Office Recurring Deposit Rules, 1981 stipulated that the maturity period of a Recurring Deposit (RD) account should be five years. However, the depositor could at his/her option, either prematurely close the account after three years from the date of opening the account or continue the account for a further period up to a maximum of five years. Thus the total number of installments permissible was 120. Minus balances were not permitted.

An analysis of the database revealed that in four HPOs under the Delhi and Rajasthan circles, 493 accounts with deposits of Rs 34.97 lakh were allowed to be closed before three years as shown in Annexure-VIII. Further, in Tallakulam HPO under the Tamil Nadu Circle, 143 cases of minus balances were noticed.

The management of the Delhi Circle stated that matter was under scrutiny while the managements of the Rajasthan and Tamil Nadu circles accepted the facts and stated that this deficiency had arisen as the transactions were being processed through the data entry module. This underlined lack of validation controls and the continuance of data entry module in violation of the instructions.

An analysis of the database in 22 HPOs in 10 circles as shown in Annexure-IX revealed that more than 120 installments ranging from 121 to 11,763 were accepted in 547 cases. The management accepted that the software was deficient as it was automatically generating multiple entries for the same account when bulk postings were done.

2.7.2.12 Non-recovery of service charges in respect of silent accounts

The Post Office Savings Account Rules, 1981 stipulated that an account in which a deposit or withdrawal had not taken place for three complete years, should be treated as a silent account and service charges of Rs 20 should be deducted from silent accounts with balances below Rs 50 on the last working day of each financial year.

An analysis of the database in 26 HPOs in eight circles revealed that in 17,835 accounts, service charges amounting to Rs 6.51 lakh had not been deducted by the software in respect of silent accounts as detailed in Annexure-X.

The local management accepted the fact and stated that the software did not have the facility for deducting the service charges and that the matter was being looked into.

2.7.2.13 Non acceptance of deposits in multiples of Rs 200 in TD accounts

The Post Office Time Deposit Rules, 1981 stipulated that deposits in a TD Account should be in multiples of Rs 50. This was enhanced to Rs 200 from July 2003.

An analysis of the database in 21 HPOs in six circles as shown in Annexure-XI revealed that there were 603 cases where deposits were not accepted in multiples of Rs 200 in spite of the provision available in the software to accomodate the denomination whenever there was any change in the rules.

The local management accepted the fact and stated that the same was being updated.

2.7.2.14 Interest not rounded off in TD accounts

The Ministry of Finance issued a notification in July 2003 to the effect that in cases where the interest in TD accounts contained part of a rupee and if such part was 50 paise or more, it should be rounded off to one complete rupee and if such part was less than 50 paise, it should be ignored.

Audit analysis of the database in nine HPOs under the Delhi, Karnataka and Uttar Pradesh circles revealed that the software did not incorporate the provision of rounding off. The local management accepted the fact.

2.7.2.15 Subscription in more than 12 instalments in a year in PPF accounts

Rule (5) of the PPF scheme stipulated that the subscription for any year should be paid into the account in one lump sum or instalments not exceeding 12 in a year.

An analysis of the database of 38 HPOs in 11 circles revealed that in 600 accounts, subscriptions were made by customers in more than the prescribed number of installments as shown in Annexure-XII. On this being pointed out, the Postmaster, Rajasthan Circle stated that the faults had occurred due to entry through the data entry module and that the excess installments would be regularized. The reply was not tenable as the collection of extra installment was irregular and the maximum that could be done at this stage was not to allow any interest on these extra installments.

2.7.2.16 Non Recovery / Short Recovery of Default fees.

Rule 7 (2) of the PPF Scheme 1968, stipulated that a subscriber who failed to subscribe in any year according to permissible limits, could approach the Accounts Office for condonation of the default, on payment, for each year of default, a fee of Rs 50* along with arrears subscription of Rs 500* for each year.

Analysis of the database in seven HPOs in the Delhi, Karnataka and Rajasthan circles revealed that in 1693 cases, an amount of Rs 0.28 lakh towards default fee had been recovered short or not recovered at all. In the Delhi and Karnataka circles, in 250 cases, arrear subscriptions amounting to Rs 0.78 lakh had not been realized from the subscribers. The software did not have any provision to indicate the correct amounts to be collected in these cases.

The local management accepted the fact and stated that this would be examined.

2.7.2.17 Inadequate details in the database of National Savings Certificate

The National Savings Certificates (NSC) purchased by customers were eligible for encashment after six years. In New Delhi GPO, it was observed that the database had details of only the certificates purchased after 16 January 2003. On account of this, whenever a customer presented a certificate for encashment of maturity value, the same was being done manually. This indicated that the switchover to computerization and capture of historical data was not implemented properly.

Further the software had an inbuilt feature for updating the database pertaining to lost/stolen certificates. Audit scrutiny in Puri HPO under the Orissa Circle revealed that the list pertaining to lost/stolen certificates had not been updated in the database. It was observed that a case of fraudulent encashment of KVP certificates amounting to Rs 6.06 lakh had occurred, which could have been avoided had the list been updated. On this being pointed out, the Postmaster accepted the facts. Similar instances of non-updation of negative list showing lost/stolen certificates in the database were noticed in the Bihar Circle also. This showed that the facility available in the software was not being utilized.

2.7.2.18 No provision to distinguish between loan and withdrawal in PPF

Rule 9 of the scheme stipulated that withdrawals from the PPF scheme were permissible only after five years from the end of the year in which a subscriber made the initial subscription.

Analysis of the database in two HPOs in the Karnataka Circle revealed that in 60 cases, withdrawals were availed by the subscriber before the expiry of

* prior to 15-11-2002 the rate was Rs 10
* earlier Rs 100

five years. The transaction type code assigned by the software for both loans and withdrawals were 'W' whereas there should have been different codes for loans and withdrawals. On this being pointed out, the Postmaster of Dharwar stated that the cases were to be checked to ascertain whether they pertained to loans or withdrawals, and admitted that the software needed to have adequate validation to distinguish between a loan and a withdrawal.

2.7.2.19 Deficiency in conversion of MIS accounts

The Monthly Income Scheme (MIS) rules permitted the conversion of a single MIS account into a joint account and vice versa. However, audit scrutiny revealed that when a joint account was converted into a single account, the software did not ensure adherence to the maximum monetary limit pertaining to the single account status. As post maturity interest was permitted on the amount due for a minimum period of two years from the date of maturity to the date of repayment and was to be calculated at the simple interest rate applicable from time to time for SB accounts, but, the software did not have any provision to calculate post maturity interest, the work was being done manually, defeating the objective of computerization. The Management accepted the fact and stated that the software was deficient in this regard.

2.7.2.20 Non-Incorporation of Income Tax Guidelines

All banking companies are governed by directions issued by MoF. In May 1996, DoP issued instructions to all circles to furnish information in respect of post office customers making withdrawals of Rs 50,000 or more (enhanced to one lakh in July 1999) to the Income Tax authorities. Further amendments were made in the Income Tax Act, by the MoF, requiring Permanent Account Numbers (PAN)/General Index Reference (GIR) numbers for transactions beyond the limit of Rs 50,000 or Rs 1 lakh. MoF in October 2004 issued a clarification to DoP to adhere to the instructions issued by it.

Audit observed that DoP did not include these requirements for generating tax reports in the URS. Further, the software did not have the facility to accept GIR numbers or PAN, till date, nor did it have any provision to generate reports required for transmission to the Income Tax Department. Audit observed that in the source document itself (Form SB-3) used for opening of an account, provision for capturing the particulars of PAN/GIR numbers did not exist.

Incorporation of these features in the software would not only have fulfilled the obligations towards the tax authorities, but also minimized manual work. It would also have prevented the opening of multiple accounts by individuals exceeding the prescribed limit in all the post offices across the country as PAN numbers were unique. Besides, the software did not have a provision for deduction of tax at source.

2.7.2.21 No provision for payments through cheque

Amounts due to customers could be paid either by cash or cheque. DoP had instructed that if the maturity value was Rs 20,000 or more, the payment should be made by cheque as provided in Section 269-T of the Income Tax Act.

Audit analysis revealed that a cheque-writing module was not integrated into the software, which could enable writing of cheques whenever the withdrawal amount was Rs 20,000 or more.

Recommendations :

- **DoP should re-engineer the software to automatically uninstall the data entry module once the online module is utilized.**
- **Databases should be regularly validated by IT trained internal audit teams on a periodic basis.**
- **DoP should ensure complete incorporation and availability of POSB rules in the software.**
- **DoP should ensure that the software has a provision to generate error reports based on process validation to minimize inaccuracies in the database.**
- **DoP should consider redesigning its source document i.e. application for opening an account, enabling it to capture all details.**
- **DoP should place the details of lost certificates on its website so that it not only benefits its post offices but also the general public as well as other banks so that these are not fraudulently mortgaged.**

2.8 INADEQUACIES IN THE SYSTEM DEVELOPMENT METHODOLOGY

The inadequacy of validation controls in the Sanchay Post software as pointed out above could have been identified and rectified at the time of the development of the software had all the stages of system development like user requirement specification, testing and implementation been followed meticulously. The shortcomings in the system development methodology adopted for developing the software are discussed in the following paragraphs:

2.8.1 Deficiencies in User Requirement Specification (URS)

Specification of the user requirements was one of the most important stages in the development of software, where the validation controls and business rules should be adequately specified. Audit examination of the URS submitted by the vendor and approved by DoP revealed that the required validation controls

were not specified adequately, which resulted in deficiencies in the functioning of the software as pointed out in paragraph 2.7.

DoP performed the savings bank functions either directly or through the authorized agents. Audit, however, observed that the three main agency functions, namely, the Standardized agency system, the Public Provident Fund agency system and the Mahila Pardhan Kshetriya Bachat Yojana agency system had not been included in the URS and till date, these functions were not incorporated in the software. As a result, savings bank operations involving payment of commission to the agents and tax deduction at source were carried out manually, defeating the objective of complete computerization of savings bank operations.

2.8.2 Testing and Implementation

Any software should be stringently tested for its functioning before implementation to ensure it suited the business requirements of the organization. The Sanchay Post software was tested by the Postal Training Centre (PTC) Mysore in March 1998 and M/s Datanet Corporation delivered the software after incorporating the modifications suggested by PTC Mysore, to the initial 180 sites in August 1998. The software was declared fully operational by PTC Mysore in January 1999 after the vendor had carried out further modifications as suggested by them. DoP procured additional 115 and 50 copies of the software in March 1999 and March 2000, respectively.

However, scrutiny in audit revealed that in December 2000, PTC Mysore had intimated DoP that the software suffered from programming bugs, logical errors and functional inconsistencies of a very serious nature. By this time, DoP had already purchased 345 copies out of the total 445 copies. Again in March 2001, PTC Mysore communicated to DoP that no further purchase orders should be placed on M/s Datanet Corporation till a third party validation of the software was carried out. In spite of this, without ensuring rectification of the deficiencies pointed out by PTC Mysore, DoP went ahead and placed another purchase order for 100 copies of the software on M/s Datanet Corporation in March 2001.

This showed that while the testing process itself was flawed at the initial stages, the recommendations of the testing authority restraining further purchases till proper validation was achieved, were also not adhered to. The instances of lack of validation controls and deficient functioning of the software as pointed in paragraph 2.7 should have been addressed at the stage of testing and implementation.

2.8.3 Lack of connectivity with the existing software

One of the important considerations at the time of introduction of a new software was to ensure its compatibility with the existing software. The purchase order placed on M/s Datanet Corporation for supply of the software stipulated that it should have the facility for connectivity with the software which was being

used by Savings Bank Control Organisation (SBCO) for internal check purposes and other software such as NIC UNIX, Oracle, ITI OASIS and APS SB which were in existence, before the introduction of Sanchay Post.

Audit observed that even after seven years of the introduction of Sanchay Post software, it lacked

- proper connectivity with the software in use by SBCO; and
- the ability to exchange data between Head Post Offices and Sub Post Offices, as also from institutions and bulk account holders electronically both by using modems and TCP/IP* mode as well as through floppies.

These deficiencies resulted in duplication of data entry and inadequate monitoring by SBCO.

Recommendations:

- **DoP should adopt an IT system development methodology which should, *inter alia*, include detailed steps to be followed for stages like project initiation, user requirement specifications, system requirement specifications, system design and acceptance testing, for any new software development or modification to existing software.**
- **A third party should validate the software as PTC Mysore had raised serious doubts about it.**
- **DoP should ensure inter-connectivity to facilitate data transfer between various offices.**

2.9 IT SECURITY AND BUSINESS CONTINUITY

IT security controls and business continuity plan were critical for the efficient functioning of the software since the savings bank operations involved financial transactions and the security of the data was of prime importance. The deficiencies observed in audit with regard to IT security and business continuity are discussed below.

2.9.1 Information technology security issues

DoP issued detailed IT security instructions only in August 2004, covering physical security, system and software security, internet based security concerns and confidential matters. The heads of offices and inspecting officers were made responsible for ensuring the implementation of these instructions.

* TCP/IP – Transmission Control Protocol / Internet Protocol – mode of exchange of data through internet

Audit examination revealed that these instructions, which were crucial to the functioning of the software, were not adhered to as

- the annual maintenance agreements for hardware had not been entered into, to mitigate the risk of system failure;
- logical security features like automatic and permanent disconnection of logon-ID in case of entry of a wrong password more than three times, automatic time out of unattended terminals and acceptance of minimum eight character passwords were not available in the software ;
- duties of system administrator were being performed by persons other than the head of the office; and
- anti virus software installed was not being updated regularly.

2.9.2 Non formulation of business continuity and disaster recovery plan

A business continuity and disaster recovery plan is a crucial component of an enterprise's risk management process.

Audit examination revealed that DoP had not formulated any business continuity and disaster recovery plan. DoP's instructions only stipulated regular backup of data and its storage in an offsite location, but did not include the storage of application and systems software and their regular testing to ensure that the backup data could be relied upon.

2.9.3 Technological change requirements affecting business continuity

Improvement in the operating system software is a continuous process as newer versions are released by vendors from time to time. It was, therefore, important that the Management was aware of these new technologies for ensuring utilization of the current version of the software which would avoid the risk of using an obsolete version, no longer supported by the vendors.

The operating system (OS) which was initially specified for Sanchay Post was Windows NT and the RDBMS was MS SQL server 6.5. Audit scrutiny revealed that out of 82 locations, the latest versions of the OS i.e., Windows 2003 server was available in nine locations and MS SQL server 2000, RDBMS in 34 locations. In the rest of the locations, older versions of OS like Windows NT and MS SQL 6.5 were being used as detailed in Annexure-XIII. Audit observed that Microsoft Corporation had posted notices on its web site in September 2001, regarding phasing out of Windows NT and not providing support, as also phased migration from Windows 2000 to the Windows 2003 server. In such a scenario, in case of malfunctioning of the operating system, support from the vendor would not be available. This would adversely affect the continuity of business services.

Recommendations:

- **Backup procedures should include copies of application and operating system software, and these should be placed at off-site locations. The instructions should be modified to include regular testing of back up data.**

- **Business Continuity and Disaster Recovery Plan should be formulated and circulated widely.**

- **DoP should conduct a study on the open source options available for operating systems which would cut its overhead costs.**

2.10 BUSINESS NEEDS NOT ADEQUATELY ADDRESSED

For a software to be constantly effective, it should keep pace with the changing business needs. In the case of DoP, this meant that the computerization of savings bank operations was extended to more number of post offices; proper change management systems were in place; more operator friendly features were introduced in the software and the feasibility of providing better services to the customer through inter linking of post offices was explored. Audit, however, observed that DoP had not taken sufficient action to address these issues as discussed below.

2.10.1 Slow pace of computerisation

The main objectives of computerisation of post offices were the transformation of the India Postal System through the induction of this technology and achievement of a level of excellence, which would make it truly world class. The computerisation of the SB branch was expected to result in better efficiency, greater customer satisfaction, fast and effective counters, computerized records and returns on SB.

There were 842 Head Post Offices and 27,711 Sub Offices apart from 127119 Branch Post Offcices (March 2004) across the country. Further, as per the targets of the Tenth Five Year Plan, 842 Head Post Offices and 8,000 Sub Post Offices were to be totally computerized. However, even after seven years of its introduction, DoP had procured the software for only 445 sites, which was less than five *per cent* of the target of 8,842 post offices. This was indeed very slow progress especially considering the fact that the revenue earnings for SB working had increased from Rs 969.87 crore in 1998-99 to Rs 2,029.82 crore in 2004-2005.

2.10.2 Inadequate change management

After introduction of any software, it was the responsibility of the Management not only to constantly monitor the functioning of the software, but

also to analyse and ensure that the software was correspondingly modified to function in tune with the latest changes in business rules.

The module for the Senior Citizens Savings Scheme introduced in 2004 had not been added to the software. This resulted in the simultaneous functioning of the computerized and the manual system, defeating the objectives of computerization.

Further audit examination of the purchase orders placed by DoP on M/s Datanet Corporation for procurement of the Sanchay Post software revealed that:

* no provision existed for incorporation of modifications in the software on introduction of new schemes and changes in rules;

* there was no clause which indicated that installation of the latest version being purchased would also cover its implementation in the sites where the software was already in use.

The above indicated lack of effective change management.

Source Code

The terms and conditions of the bid document required the bidders to submit the quote for delivering the source code. M/s Datanet Corporation had agreed to sell the source code to DoP with the condition that the executable copies would be deployed only after payment of licence fees. Audit analysis revealed that the condition regarding supply of the source code had been incorporated in each of the four purchase orders placed, which implied that four copies of different versions of the software source code should have been available with DoP. However, it was observed that only one copy of the source code was supplied to DoP in 1999, whereas the latest version 4.5 was released by M/s Datanet Corporation in January 2003. It was also seen that the software had been developed in a special framework called the Business Process Automation System (BPAS), which was a proprietary item of M/s Datanet Corporation. DoP could not improve or extend the software without this framework. This deficiency rendered the DoP totally dependent on the vendor for all future improvements in the software.

2.10.3 Operator friendly features not available

Any software should be operator friendly so that there were minimal delays in completing transactions. As per Rule 35 of POSB Manual Vol-I, the counter assistants were authorized to accept deposits and permit withdrawals up to Rs 2,000 in order to provide instant counter service. Audit, however, observed that transactions below Rs 2,000 were also required by DoP to be authorized by the supervisor, thereby defeating the purpose of instant counter service. Further, the software did not

- facilitate automatic transfer of maturity value of RD accounts to SB accounts,
- facilitate automatic crediting of maturity value of TD accounts to SB accounts,
- facilitate credit of TD interest to SB/RD accounts,
- make pass book printing and electronic signature scanning functional, and
- have any complaint monitoring mechanism incorporated in it .

This meant that the customers were being deprived of instant counter service.

2.10.4 Non linking of post offices

The Sanchay Post software was developed to work in a Local Area Network environment within a post office in spite of the fact that DoP had 1.55 lakh post offices with a customer base of 11 crore account holders throughout the country with annual deposits exceeding Rs 25,000 crore in 1998-1999.

The POSB rules provided for opening of a number of SB, MIS and PPF accounts by individuals within the prescribed limits and with certain conditions. It was difficult to implement some of these rules in a manual environment, where there was no interconnectivity between different post offices. DoP should attempt to interlink its post offices to

- implement its rules such as restricting an individual from opening account(s) in excess of Rs 1 lakh in SB and Rs 3 lakh in MIS in all post offices and investing over Rs 70,000 in PPF in a year; and
- provide customers access to their accounts through the internet and any time any where service for greater customer satisfaction and thereby attracting more customers.

This is all the more important as customer base had risen to 14 crore account holders with annual deposits exceeding Rs 97,000 crore in 2003-2004.

Recommendations :

- **DoP should speed up the process of computerization and introduction of banking software in all its post offices, which will help it in providing all round services. It should also explore the possibility of going in for a centralized banking software.**

- **DoP should have a well documented change management mechanism in place to handle changes in software requirements and incorporation of changes in rules.**

- **DoP should explore inter-connectivity of each post office, and utilize its network of post offices through adoption of web-based technology to provide 'any time any where' banking services.**

2.11 CONCLUSION

The objective of computerisation of postal savings bank functions through the Sanchay Post software was to reap the benefits of Information Technology to improve the operational performance, besides providing error free and faster service to the customers. However, even after seven years of its functioning, the software had been introduced in only five *per cent* of the post offices. As pointed out in the report, lack of sufficient validation controls along with inadequate monitoring could not adequately mitigate the major risks such as irregular opening of accounts, irregular deposits and payment of undue interest. The deficiencies in system development and implementation and IT security and business continuity together as well as the failure to address the changing business needs pointed towards lack of effective monitoring of computerization and ineffectiveness of the software. DoP should address these inadequacies urgently, review the functioning and controls in the present software and move towards a centralized networking system of post offices in order to achieve higher and higher levels of excellence.