CHAPTER 2
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

DEPARTMENT OF POSTS

IT Audit of Computerised Postal Life Insurance System

Highlights

The Department of Posts introduced the Computerised Postal Life Insurance System in all the postal circles during 1990-91 to 1996-97 but the system had not stabilized even after eight years of the completion of the computerisation.

The system failed to incorporate Departmental rules/checks in a number of areas such as capturing of details of policy-holders for the purpose of calculation of premia and reconciliation, thereby exposing itself to risks of improper monitoring, double payments, frauds, etc.

The system lacked data integrity due to deficient internal controls as the 'validation checks' were inadequate in respect of critical inputs required for calculation of premia, monitoring of loans, capturing of policy details, etc.

IT security related control measures in place were not adequate.

Reliance on manual work continued and the objectives set by the Department for introduction of the package such as reducing paper work, eliminating duplicate entries and providing a user-friendly and error-free work environment are yet to be fully realised.

List of recommendations

- ***DoP should review the system and incorporate the Departmental rules/checks, wherever lacking. DoP should also involve their Internal Audit wing in this exercise.***
- ***A mechanism should be formulated to ensure that any changes in policies and instructions are immediately incorporated in the system.***
- ***Necessary internal controls should be incorporated, so that the attendant risks of incorrect calculations and postings of premia, incorrect payment of claims, incorrect repayments of loans, etc are eliminated.***

- ***DoP should resolve all the pending issues with NIC, which had developed the system for ensuring adequate support to the system.***
- ***The implementation of IT security related controls should be reviewed to eliminate risks of manipulation and loss of data. It should also prepare a detailed disaster recovery and business continuity plan and ensure its strict implementation.***

2.1 Introduction

The Department of Posts (DoP) introduced the Postal Life Insurance (PLI) scheme as a welfare measure for the employees of the Postal Department in 1884. In course of time, it extended the scheme to employees of other Central Government departments, state governments, public sector undertakings, local bodies, banks, etc. As of March 2004, PLI had a total business of 22.09 lakh policies with a total assured sum[1] of Rs 15,917.61 crore. The PLI scheme offers five types of policies, the details of which are given in **Annex-I**.

2.2 Organizational setup

DoP carries out the PLI scheme as an agency function on behalf of the Ministry of Finance. The PLI Directorate, in New Delhi is headed by a Chief General Manager. He is responsible for policy decisions and control over the PLI fund and organization; procurement of business and appointment of agents. The Director, PLI, Kolkata is responsible for central accounting of receipts and payments of the PLI fund.

The PLI section in each circle is under the overall control of the head of the circle, who is assisted by a Director of Postal Services. The Assistant Postmaster General/Deputy Divisional Manager, in-charge of the PLI section in a postal circle, is responsible for procurement of business; settlement of claims; appointment of agents and monitoring of publicity and marketing.

2.3 Computerised Postal Life Insurance System

The Computerised Postal Life Insurance System (CLIP) was developed by the National Informatics Centre and installed in all the circles during 1990-91 to 1996-97. The system uses *Oracle* software on a *Unix operating system platform*.

The objective of the package was to computerise all the functions of PLI such as proposals, posting, maturity, loans, surrenders, etc. It aimed to provide better customer services, an improved management information system, faster and smoother system performance and enhanced security.

[1] assured sum - the maturity value of a policy.

The CLIP system comprises ten modules. These are (i) **Proposals** (for entering data in respect of new policies), (ii) **Postings** (for updating data in respect of individual policies), (iii) **Loans** (for exercising controls in respect of loans), (iv) **Maturity** (for exercising all the checks on maturing of policies), (v) **Surrenders** (for exercising checks in respect of surrender of policies), (vi) **Administration** (for administering the data base), (vii) **Print Man** (for printing various outputs), (viii) **Reports** (for generating various reports), (ix) **Master** (for creating the master data) and (x) **Customer Service** (for providing details of policies).

2.4 Scope of audit

Audit of the CLIP system was conducted during 2003-04 in 15 out of the total of 22 postal circles namely, Uttar Pradesh, Gujarat, Karnataka, Madhya Pradesh, Tamil Nadu, Orissa, Delhi, Andhra Pradesh, Rajasthan, Punjab, North East, Uttaranchal, Maharashtra, Kerala and Bihar.

The objectives of audit were to:

- ascertain whether Departmental rules had been incorporated in the system for its effective functioning;
- ascertain the effectiveness of other internal controls associated with the system;
- evaluate the effectiveness of Information Technology (IT) security associated with the system; and
- ascertain how far the objectives set by DoP for the introduction of the system were achieved.

2.5 Audit findings

During the course of audit, a number of deficiencies were observed in the CLIP system. As a result, its implementation was only partial and reliance on manual work continued. The principal deficiencies are discussed under the broad categories of inadequate incorporation of Departmental rules in the system, deficient internal controls in the system; IT security related issues and role of implementing agencies.

2.6 Inadequate incorporation of departmental rules in the system

Departmental rules ensure effective internal controls to minimise risks. A computerised system should incorporate all the relevant rules or provide for the system based controls. If these rules/controls are not incorporated in the package, risks such as improper monitoring, over payments, frauds, etc are not mitigated. This would not only necessitate manual interventions, but would also defeat the objectives of providing an error free and more responsive environment, together with the easy flow of work. This is even more pertinent in the case of PLI, which has to operate in a competitive environment.

Departmental rules had not been incorporated completely in the CLIP system, as discussed below.

2.6.1 No provision for rejection of invalid data at entry level- 'Proposals' module

The 'Proposals' module is used for entering details for starting a new PLI policy such as name, address and date of birth of applicant, type of policy, assured sum, mode of payment, date of declaration and nominee details.

A. Acceptance of invalid date of birth

The ‘date of birth’ field in the 'Proposals' module is required to calculate the age of the insurer and check his/her eligibility for opening a policy. It is one of the crucial fields on the basis of which premia are calculated. Prior to 18 August 2003, the age for entry into a new policy was between 19 and 50 years. The maximum age was revised to 55 years from 18 August 2003.

Sample checks by Audit in the Madhya Pradesh, North East, Orissa, Rajasthan and Tamil Nadu circles revealed that the system was accepting even those proposals, where the age of the applicants was less than 19 years or more than 50 years prior to 18 August 2003 and more than 55 years after 18 August 2003. In the absence of incorporation of this Departmental rule, there was a risk of entry of ineligible persons into the system.

The Management accepted the audit observation.

B. Acceptance of assured sums in excess of the prescribed limit

The assured sum is another crucial field for the calculation of premia.

Scrutiny in the Gujarat, Karnataka and Rajasthan circles revealed that the system accepted assured sums in excess of the prescribed limits, thereby exposing itself to the risk of incorrect calculation of premia.

The Deputy Divisional Manager, PLI, Ahmedabad, while accepting the facts, stated in March 2004, that action to regularise the excess assured sums as per the Post Office Insurance Fund rules had been taken. The Deputy Divisional Manager, PLI Jaipur, while confirming the facts, stated that action would be taken as per the rules.

2.6.2 No provision in the system for reconciliation – 'Postings' module

The Departmental rules for ensuring correctness of posting of premia in the individual accounts stipulate that the amounts posted in the individual accounts in the PLI section should be totalled and reconciled with the figures in the schedules containing the details of PLI recoveries made at different post offices.

The system did not have any provision for such a reconciliation. The total premia received as per the CLIP report of Delhi circle for 2003-04 was only Rs 81.56 lakh whereas the total premia received during the same period as per the schedules was Rs 23.33 crore. Similarly, the total premia received in the Kerala circle as per the CLIP report for the period 2003-04 was Rs 5.36 crore whereas the actual total premia received during the same period as per the schedules was Rs 14.75 crore.

Thus, the correctness of posting of premia in the individual accounts could not be ensured. Unless the system is able to ensure reliability of postings of premia in respect of individual accounts through reconciliation with the schedules, the correctness of the output from CLIP is not ensured.

The Management accepted the above audit observation.

The above deficiencies are illustrative and not exhaustive.

Recommendations

- **DoP should review the system and incorporate the Departmental rules/checks, wherever lacking. DoP should also involve their Internal Audit wing in this exercise.**
- **DoP should formulate a mechanism to ensure that any changes in policies and instructions are immediately incorporated in the system.**

2.7 Threats to data integrity due to deficient internal controls

The internal controls associated with a system should be such that the outputs generated are reliable. ‘Validation checks’ should be designed so that the system does not accept incorrect data and minimises business risks.

In a number of instances, the internal controls were inadequate, as discussed below:

2.7.1 Acceptance of invalid codes for modes of payment

There are only two modes of payment of premia i.e. cash payments made in the post offices or deductions from salaries. The field ‘Mode of Payment’ is to be filled in by using the alphabet ‘C’ for cash recovery or ‘P’ for pay recovery.

Sample check in the Andhra Pradesh Circle revealed that the system was accepting all characters including numerals. In the absence of adequate controls, the system was not in a position to ensure proper monitoring of payments.

Deputy Divisional Manager, PLI, Hyderabad, while accepting the facts in January 2004 stated that the work was being done manually.

2.7.2 Acceptance of invalid dates

The application form has three crucial dates i.e. the date on which the applicant signs the proposal; the date on which the applicant signs the declaration and the date on which the proposal is accepted and signed by the competent authority. The date of declaration must be on or after the date of proposal and the date of acceptance must be on or after the date of declaration.

Sample checks by Audit in the Karnataka and Orissa circles revealed instances where the date of acceptance was prior to the date of proposal; the date of entry was prior to the date of birth of the insurer; the date of maturity was prior to the date of entry; the date of entry was equal to the date of birth and the date of acceptance was prior to the date of proposal.

Unless the system is able to ensure correct capturing of details in respect of individual accounts maintained in the PLI section through rejection of the invalid dates, there were risks of incorrect calculation of premia and incorrect payments of claims.

On this being pointed out, the Deputy Divisional Manager, Bhubaneswar confirmed the facts and figures and agreed that the software should have necessary controls to reject incorrect inputs.

2.7.3 Acceptance of invalid policy status codes

Claims are processed and payments are made on the basis of the status of the policies. For the purpose of monitoring, every policy is given a status code such as ‘P’ for proposals; ‘C’ for current; ‘M’ for matured; 'S' for surrendered and ‘T’ for transferred. The default value for policy status is 'C' in the ‘policy status’ field.

Sample checks by Audit in the Andhra Pradesh, Karnataka, Punjab and Tamil Nadu circles revealed that the system was accepting invalid policy status codes such as '**.**', '**,**' and alphabets other than the default codes. Sample checks in the Orissa, Punjab and Rajasthan circles also revealed that the system was showing the status of matured policies as current. Thus, the system cannot be completely relied upon since it contains unreliable data.

The Management in the Tamil Nadu and Punjab circles stated in reply that this was due to errors made at the time of data entry and that the software lacked the required validation checks.

Recommendation

❖ **DoP should incorporate necessary internal controls, so that the attendant risks of incorrect calculations and postings of premia, incorrect payment of claims, incorrect repayments of loans, etc are adequately managed.**

2.8 Information Technology security related issues

For a computerised system to work efficiently and effectively, it is imperative that the controls related to IT security are effective and are followed scrupulously. Audit observed various deficiencies in the implementation of IT security related measures in respect of the CLIP system as discussed below:

2.8.1 Deficient password policy

The passwords used to gain access to the package and the system resources should not be easy to guess, should be changed regularly and should comprise a minimum of eight alphanumeric characters.

The password procedures consisted of the following deficiencies:

- the system accepted passwords of single character,
- the user IDs and passwords were not changed since their first creation,
- the system did not provide controls against unauthorised attempts to login,
- the system did not generate log reports on unauthorised attempts.

2.8.2 Ineffective segregation of duties

Segregation of duties ensures that officials are granted access to their respective operational areas only and they are not able to trespass upon other officials' areas of operation, especially those of their supervisors, who exercise checks over their activities.

There was no such segregation of duties and the operators had access to almost all the modules as also to the areas assigned to their supervisors. This arrangement provided scope for unauthorised changes to the data, rendering the integrity of the database suspect, with risk of manipulation.

2.8.3 Frauds due to inadequate logical access controls

Two cases of fraud came to notice in the Orissa and Rajasthan circles as a result of inadequate IT security controls in the system.

(i) In the Orissa Circle, a postal assistant, who was dealing with PLI claims, managed to generate second sanction memos in respect of two policies by changing the status of the policies and the addresses of the insurers, using the password assigned to him. The postal assistant prepared the memos in February and March 2002 for Rs 47,100/- and Rs 21,809/- respectively. The Deputy Divisional Manager, PLI approved these sanction memos without going through the related supporting documents.

The investigation report at the circle level observed that the date of payment, which was posted in the system, could be changed by any one at any time by using the password assigned to the operators, which might lead to tampering of records with fraudulent intentions. Hence, mere posting of dates of payment in the system was meaningless, unless the system was made more secure.

As per standard IT security practices, there should have been effective segregation of operational areas to deny access to operators to alter policy details, which would have prevented such frauds. Moreover, the standard practices of maintaining and reviewing the system and database access log files would have acted as deterrents.

(ii) In the Rajasthan Circle, the first case of fraud came to light while entering the date of payment in the system for the purpose of preparing reports to be sent to Director, PLI, Kolkata. The date of payment was already available in the system. It was confirmed through the Print Man module that a genuine sanction was issued by the system in December 1999. After searching the maturity index register and the case file from old records, it was found that the sanction issued in January 2001 was bogus, bearing the fictitious signature of the Deputy Divisional Manager, PLI. During the enquiry, a total of 64 cases of bogus sanctions for Rs 5.66 lakh were detected at three HPOs of Jaipur.

As per standard IT security practices, there should have been *'Validation checks'* to ensure that a second sanction was not accepted by the system unless the first sanction was cancelled by the competent authority, in order to avoid such frauds.

As illustrated above, the changing of status by anyone using an operator ID and password can lead to intentional frauds like double payments against a matured policy. Even after four years of the occurrence of these frauds, the deficiencies in the input controls of the package were persisting, leaving it open for further manipulations and fraud.

Recommendations

- ❖ **DoP should ensure that there is effective segregation of operational areas.**
- ❖ **DoP should maintain and regularly review the system and database access log files.**

2.8.4 Inadequate implementation of disaster recovery and business continuity plan

PLI functions are dependent on the CLIP system for about 22 lakh policies. The system is pivotal for its insurance operations and is a critical tool for analytical functioning of the PLI wing. Due to human error, failure on account of electric and magnetic fluctuations, natural calamities or crashing of the computerised system, the activities related to PLI can get severely disrupted. It is, therefore, imperative that DoP has a detailed disaster recovery and business continuity plan so that in case of any eventuality, operations are back to normal at the earliest with minimum losses.

DoP had issued orders for taking regular backup of data but did not have a documented disaster recovery and business continuity plan for all its computerised activities. Even the orders issued for regular backup of data were not being followed. It was also observed that the back up data were not being reviewed periodically in order to ensure that there were no problems of data retrieval. Further, it was observed that the back up data were not stored off the site in Orissa and North East circles.

The Management accepted the audit observations.

Recommendation

❖ **DoP should review the implementation of IT security related controls to eliminate risks of manipulation and loss of data. It should also prepare a detailed disaster recovery and business continuity plan and ensure its strict implementation.**

2.9 Role of implementing agencies

While the PLI Directorate monitors the PLI functions and the CLIP system, NIC, which developed the system, is expected to provide support to the system for its smooth operation by offering software solutions to various errors and difficulties being reported at different stations. The system had not stabilized even after eight years of completion of the computerisation due to various deficiencies. One of the major reasons for the same was inadequate support provided by NIC.

The PLI Directorate stated in August 2004 that the support extended by NIC was ad hoc and changes required in the system had not been adequately implemented by NIC.

Recommendation

❖ **DoP should resolve all the pending issues with NIC for ensuring adequate support to the system.**

2.10 Conclusion

DoP introduced the CLIP system in all the postal circles by 1996-97. However, the system has not stabilised even after eight years of completion of the computerisation due to incomplete incorporation of Departmental rules and weak internal controls. IT security related control measures in place are deficient. The support provided to the system by NIC is inadequate. As a result, reliance on manual work continues. There is an urgent need for the department to take immediate remedial measures to stabilise the system so that the intended benefits of computerisation of PLI activities can be fully realised.

The matter was referred to the Ministry in October 2004; their reply was awaited as of February 2005.