



2.1.7 Conclusion

The IT security of the computerised applications in Western Railway was grossly inadequate. Neither a comprehensive IT security policy was developed nor were the risks and vulnerabilities assessed. The network security and network traffic was not effectively monitored, information security and access controls were inadequate to protect the confidentiality, integrity and availability of the systems and data thereby exposing the IT systems to both external and internal threats.

2.2 Provident Fund Accounting System in Izatnagar Division of North Eastern Railway

2.2.1 Highlights

Business rules relating to accounting of Provident Fund transactions were not fully incorporated in the Provident Fund Accounting System in Izatnagar Division of North Eastern Railway leading to incorrect processing of transactions.

(Para No.2.2.6.1)

The Provident Fund Accounting System was not functioning concurrently with the Pay Roll System and therefore up to date balances of subscribers' PF accounts were not available.

(Para No.2.2.6.2)

Validation controls were deficient, which adversely affected the reliability of data. IT Security policy was not framed and weak access control mechanisms coupled with absence of audit trail rendered the Provident Fund Accounting System vulnerable to manipulation.

(Para Nos.2.2.6.3 and 2.2.6.4)

2.2.2 Recommendations

- North Eastern Railway Administration should modify the Provident Fund Accounting System to incorporate all the business rules relating to PF accounting. The system should also be integrated to function concurrently with the Pay Roll System.
- The deficiencies in validation pointed out should be rectified on priority. North Eastern Railway Administration should strengthen Information System security by drawing up a comprehensive IT Security policy and by strengthening logical and physical access controls.

2.2.3 Introduction

To facilitate correct and updated maintenance of Provident Fund (PF) accounts of 10,331 employees and payment of miscellaneous bills, North Eastern Railway Administration implemented computerised Provident Fund (PF) Accounting System in August 1998, at Izatnagar Division. The system is operational in the Divisional Accounts Office, Izatnagar under the control of Senior Divisional Financial Manager with 12 nodes connecting with one Pentium server on DOS platform and dbase as application software.

2.2.4 Audit objectives

Audit of the P.F. Accounting System implemented over Izatnagar Division of North Eastern Railway was conducted with a view to assessing whether the:

- System was developed in accordance with extant rules and provisions and data was reliable.
- Information System security was adequate and effective in regulating the IT environment.

2.2.5 Audit scope, criteria and methodology

IT Audit of the PF Accounting System was conducted for a period of four years and records for the period from 2004-05 to 2007-08 were examined. The extant rules and provisions in the railway codes were used as audit criteria to evaluate the system. Apart from examination of relevant records, data analysis was also carried out to arrive at conclusions.

2.2.6 Audit findings

The Information Technology audit of PF Accounting System implemented in Izatnagar Division of North Eastern Railway disclosed that the system was not designed as per business rules. Validation controls and Information System security were deficient, which adversely affected the integrity of data processed as brought out below:

2.2.6.1 Non mapping with business rules

Audit observed that business rules relating to accounting of Provident Fund transactions were not fully incorporated in the system leading to incorrect processing of transactions as shown below:

- Even though the rule provides that recovery of temporary withdrawal from Provident Fund should commence from the month following the month in which it was sanctioned, the provision was not built in the system. Consequently, it was noticed that the system could not commence monthly recovery from December 2004 for temporary withdrawals from Provident Fund sanctioned in November 2004 for 16 employees.
- As per provisions in the code, interest should not be granted to an account after six months of superannuation even if the final settlement on superannuation had not taken place. There was no inbuilt control to restrict the payment of interest up to six months of the date of superannuation.
- The subscription to PF should be rounded off to the nearest rupee, fifty paise and above being counted as the next higher rupee and less than fifty paise being dropped. Due to incorrect logic built in, the system was rounding off fractions of more than fifty paise only to the next higher rupee, which was inconsistent with the rule. It was observed that in the month of March 2005 and February 2006, there were 29 and 32 cases respectively where fifty paise was not rounded off to the next higher rupee. Only more than fifty paise was rounded off to the next higher rupee which resulted in less recovery.
- In PF Module, the length of the amount field of Voluntary Provident Fund (VPF) was fixed at four digits ('9999'). Though admissible by rules, the system could not capture the actual contribution towards VPF of seven employees in February 2006, whose contributions ran into five figures i.e.; more than Rs.9999.

2.2.6.2 Delayed PF Accounting

The system was not functioning concurrently with the Pay Roll System and was trailing behind by three months. In the absence of simultaneous operation of both the pay roll and PF Accounting systems, up to date balances of subscribers' PF accounts were not available.

2.2.6.3 Deficient validation checks

Audit observed that validation controls were deficient, which adversely affected the reliability of data as shown below:

- Details of subscription to PF, withdrawal from PF and interest accrued on PF of an employee are maintained through a unique Account number. Analysis of PF data revealed that in 50 cases the same PF number was

allotted to more than one employee. Presence of such duplicate PF account numbers rendered the database unreliable with possible incorrect account of employees' contributions.

- Analysis of data revealed that opening balance for 293 accounts for 2005-06 and 17 accounts for the period from 2000-01 to 2005-06 were shown as zero and minus respectively.
- The date of birth and date of appointment fields were left blank in 310 and 294 cases (February 2006) respectively. Since PF rules provide that subscription of PF deduction of an employee should commence after completion of one year of service and should be stopped three months prior to the month of superannuation, capturing data in these fields was essential to ensure adherence to rules.
- Rules state that the minimum amount of subscription payable for any month shall be 8.33 per cent of the subscriber's emoluments (Basic Pay + Dearness Pay) and shall not exceed the emoluments. Instances of irregular contribution towards PF were noticed due to inadequate validation controls. In five cases the subscription to PF exceeded the basic pay plus dearness pay drawn for the month. In 85 cases the employees' subscription towards PF (March 2005) was less than the statutory minimum.
- As per New Pension Scheme, 10 per cent of Basic pay, Dearness Pay and Dearness Allowance has to be recovered from all Railway employees who joined after 1 January 2004. This recovery should be effective from the month after the month of joining. It was observed that due to poor validation, subscriptions to New Pension scheme were not effected in 62 cases even after completion of requisite length of service.

2.2.6.4 Information System security

Information System security comprising a well documented security policy is essential to protect data and valuable assets against loss, misuse and damage to the computer system as well as to prevent the unauthorised disclosure of confidential data. There must be a well documented plan for business continuity and data recovery, definite responsibilities in accordance with rules and structures for continuing operations in the event of any intentional or unintentional disaster. Audit observed that PF Accounting system suffered from the following deficiencies:

- The control procedures were not manualised.
- Training was not provided to employees regarding operation of system and security awareness.
- User ids and passwords were shared by the users irrespective of their duties.
- No audit trail was maintained.
- To maintain data integrity, edition/deletion of data was required to be authorised at higher level. It was observed that data entry was being done

in dbase software where edit/delete facility was available to all users and all users were authorised to access the software as well as data.

- All system changes should be authorised at appropriate levels, tested and documented. It was observed that changes made in the database/system were not documented.

2.2.7 Conclusion

The PF Accounting System in Izatnagar Division of North Eastern Railway was not comprehensively developed as all the relevant business rules were not incorporated and the system suffered from inadequate validation controls. There was no IT security policy and weak access control mechanisms coupled with absence of audit trail rendered the system vulnerable to manipulation.

(N.R. RAYALU)

New Delhi

Deputy Comptroller and Auditor General

Dated:

Countersigned

(VINOD RAI)

New Delhi

Comptroller and Auditor General of India

Dated: