CHAPTER 1

Southern, South Eastern: Information Technology Audit of PRIME and Western Railways

1.1 Highlights

The application was only partially implemented in Southern, South Eastern and Western Railways. Many of the 18 sub-modules developed under PRIME were not put to use resulting in sub optimal utilisation of the application. Southern Railway was not fully equipped for implementation of the application and consequently accepted the software even though nine out of 18 sub modules had not been implemented.

(Para 1.5.1)

Southern Railway incurred an avoidable cost of Rs.2.70 crore on duplication of network facilities and operation management costs.

(Para 1.5.3)

Retention of excess manpower at EDP Centre, Chennai, in spite of the reduction in workload, resulted in extra expenditure of Rs.2.41 crore for the period from October 2001 to March 2005.

(Para 1.5.4)

General controls such as system security, IT policy, Disaster Recovery Plan were weak.

(Paras 1.6.1 and 1.6.3)

Audit trail features, providing a map for retracing the flow of a transaction, were disabled in Southern Railway and Western Railway.

(Para 1.7.1)

Inconsistencies existed in the system due to poor input validation controls and processing controls and the risk of reliance on the system was high.

(Paras 1.7.2 to 1.7.5)

Non-incorporation of rules and not updating changes in the system resulted in irregular recoveries from employees.

(Para 1.7.4)

1.2 Introduction

This chapter covers the issues arising out of IT Audit of a computerised application - Pay Roll and Independent ModulEs (PRIME) in three Zonal Railways - Southern Railway (SR), Chennai, Western Railway (WR), Mumbai and South Eastern Railway (SER), Kolkata.

PRIME was initially developed by Southern Railway, Chennai as a pilot project, as a part of the scheme of Railway Board to implement a uniform online payment and accounting system all over Indian Railways. The application was developed and implemented (April 2000), by outsourcing to M/s Faculties India Systems Services Pvt., Ltd. Bangalore (now M/s FI SOFEX) at a cost of Rs.23 lakh. PRIME was designed and developed for

distributed processing in Oracle, Developer 2K (front end) and SCO UNIX (operating system). The processing of transactions on the system could be done either on-line or at designated central locations in batches. The application was designed to monitor various career events of railway employees and to serve as a decision support system for human resource management apart from generating different establishment bills and monitoring recoveries from employees. The focus of IT audit review in the three Zonal Railways (SR, WR and SER) was assessing the control environment in which the applications software was being run, along with its adequacy and effectiveness. Analytical review coupled with substantive testing using CAATs (Computer Assisted Audit Techniques) tools viz IDEA (Interactive Data Extraction Analysis) and MS Excel was conducted to assess the reliability of the data processed and produced by the system.

1.3 Audit objectives

Audit of PRIME implemented over Southern Railway, Western Railway and South Eastern Railway was conducted to assess

- the comprehensiveness and effectiveness of systems developed;
- the adequacy and effectiveness of general controls that apply over the range of applications that run in a computerised environment; and
- the adequacy and effectiveness of application controls and whether the system was operating in accordance with the designed objectives and extant rules and regulations.

1.4 Scope and methodology

The scope of audit encompassed the evaluation of the application through a test check of records of IT and Electronic Data Processing (EDP) centres. In addition, substantive tests were also carried out by employing CAATs (Computer Assisted Audit Techniques) like IDEA (Interactive Data Extraction and Analysis) and MS Excel.

1.5 System development and implementation

Audit observed that the IT implementation strategy, planning and monitoring mechanism in place was inadequate, which led to a fragmented approach in customizing and implementing the application. Inefficient contract management on the part of zonal railway administration was also noticed. Avoidable expenditure was incurred on creation of an additional network and operation of excess manpower as shown in the following paragraphs.

1.5.1 Deficient customisation and implementation

PRIME consists of three main modules viz., Railway employees information system, employees payments system and certain independent modules with 18 sub-modules[1]. The progress of implementation of various modules of PRIME

[1] **Career Events, Personal Data, Annual Increments, Seniority, Cadre Review, Leave Accounting, Quarters, Loans & Advances, Attendance, Running Allowance, Misc. Earnings & Recoveries, Installment Based Recoveries, Fixed Recoveries, Income Tax,**

was slow and implementation of all the modules was not complete even five years after acceptance of the software in April 2000.

* In Southern Railway (SR), nine sub-modules[2], which were developed and supplied by the vendor, were not implemented so far (March 2005). While admitting the non-implementation, SR stated that the various sub-modules had to stabilise and all departments provided with trained personnel to handle the new software before allied and fresh modules could be implemented. The response of the railway administration cannot be accepted as efforts to define staff training needs and appropriate deployment of trained personnel should have been made along with development of the application.

* SR was not fully equipped for implementation of the application and as a consequence was left with no option but to accept the software even though nine out of the 18 sub-modules were not implemented. This not only limited the utility of the application but also prevented imposition of the warranty clause, which was valid only for a period of 12 months after the date of acceptance (April 2000). Further, due to non-implementation of modules such as Loans and Advances, Quarters and Leave Account, checking the recoveries of various loans and advances, interest thereon, grant of transportation allowance, recovery of rent, water charges and electric energy were carried out manually by various departments in Headquarters. Test check revealed an overpayment of allowances, short recovery and non-recovery of dues to the extent of Rs.5.59 lakh during the periods 2002-03 and 2003-04, which could have been avoided had the application been fully implemented. Even the modules implemented so far were not integrated properly thus diluting the purpose of development of the system. On the matter being taken up in Audit SR attributed the overpayments etc. to data entry failures and replied that the utility of the software was not compromised since it was properly tested and that the warranty covered 'major modules' like payroll which was already implemented successfully and the balance were only subsidiary modules which were also being implemented one by one. The reply still does not address the fact that non-implementation of certain module and sub-modules even after five years was a compromise with the planned functional aspects of the system, thus necessitating manual interventions.

* In Western Railway (WR) the application was planned for customization and implementation in WR Headquarters by August 2001. As the implementation was not completed till November 2001, WR entered into a fresh contract (April 2002) with the same firm (FI SOFEX) for completion of only two out of the 18 modules viz. Payroll and Leave, within a period of six months. Thereafter, pursuant to the decision of Railway Board to implement PRIME in WR Head quarters

---

Regular Payroll Process, Supplementary Employee Bills, Dearness Allowance Arrears and Productivity Linked Bonus.

[2] **Career events, Seniority, Cadre Review, Attendance, Running Allowance, Installment based recoveries, Leave Accounting, Quarters and Loans and Advances.**

and two of its Divisions (Mumbai Central and Vadodara) in a phased manner by July 2002, WR assigned the work of Mumbai Central Division to the same firm in June 2003 without stipulating any completion period. The implementation of the application in Headquarters and Mumbai Central Division was completed partially by August 2003 and December 2004, respectively. Customization and implementation in WR Zonal Headquarters, therefore, took more than three years and partial completion of its extension to one division took another one year. In Vadodara Division, the implementation of PRIME was yet to be undertaken. Railway Board, in December 2004, however, accorded sanction for implementation of PRIME in all other divisions of Western Railway by February 2005. The extension of PRIME to other divisions was yet to be implemented. Thus, the application has largely remained unimplemented even after lapse of four years since its planned implementation in August 2001.

* In South Eastern Railway (SER), after customization of the application, only two modules viz., Payroll and Income Tax have been implemented fully during 2003 in Head Quarters, Garden Reach, Kolkata. Till date no further modules have been implemented and the administration has not fixed any target date for implementation of PRIME.

1.5.2 Non availability of documentation

Special terms and conditions of contract signed by Southern Railway with the vendor provided that each application or module would be tested initially at the vendor's site with the test data supplied by Railways and after installation, the system would be tested with the same test data at the railway site and the results of the two sets would be compared. However no documents in support of the required tests were available for verification. SR contended that though the tests were carried out to the satisfaction of the leader of the System Development Team, no written records were maintained in the absence of any direction on maintaining evidence. SR added that as long as major discrepancies were not found in the end result on a consistent basis and as no extensive shortcomings were noted in the functioning of the modules, the objectives of design stood achieved.

The reply is not acceptable as documentation is a necessity, especially in outsourced contracts involving large sums of money, for proper evaluation of the services provided by the vendor.

Further in SR, no documentation pertaining to User Requirement Specification, System Design, Data Flow Diagram, Acceptance Test Specification etc was available in the various units where this software was customized. Non-availability of documentation affects the utility of the application. Moreover in case of a system breakdown, the users in field units would not be in a position to quickly restore the system.

Similarly in WR, except for the user manual, no other system documentation was made available to audit.

1.5.3 Avoidable expenditure towards duplication of network

In December 1998, a corporate wide information system was set up at a cost of Rs.2.6 crore between Railway Board and Zonal Railways through RAILNET – an intra railway information network. The Local Area Network (LAN) system at SR, covering Headquarters and the other two buildings, connected the important units on single mode optical fibre with a speed of 200 mbps[3] and had tremendous potential for upgradation to higher speeds including Asynchronous Transfer Mode (ATM).

Instead of upgrading the existing LAN, SR decided in October 1999 to develop another computer network, Railway On Line (ROLIN), interconnecting various buildings to exchange data relating to online application systems such as PRIME and AFRES and the project was executed at a cost of Rs.1.80 crore during June 2000. The railway administration entered into an operation management agreement with M/s. HCL at a cost of Rs.0.90 crore for a five-year period from 20 August 2001. The FA & CAO[4] (SR) had suggested optimal utilisation of the existing resources and to avoid additional expenditure at the time of design finalisation. ROLIN was, however, implemented without exploring the possibility of increased use of RAILNET. The system logs revealed that the utilisation of ROLIN ranged between 12 per cent and 18 per cent only, even at peak periods, indicating that the additional network was not justified.

SR contended that while RAILNET was meant mainly for low volume of traffic like e-mail and Internet browsing, ROLIN was a sturdy dedicated network meant for critical database comprising sensitive data. PRIME could not be made totally dependent on RAILNET and ROLIN's main 'switches' had a bandwidth of 1000 mbps whereas RAILNET backbone was a mere 10 mbps, which was grossly inadequate. SR further contended that utilisation would improve once all the modules were implemented and that costly infrastructure like ROLIN could not be expected to reach saturation level in the first year of operation and that it was installed to meet the requirements of the next five years or more.

The arguments are not tenable since the Chief Signal and Telecommunication Engineer (SR) had clearly recorded while discussing extension of RAILNET network in SR that RAILNET was designed modularly with very high bandwidth and could be expanded based on requirement by adding additional 'switches' and 'hubs'. The RAILNET backbone, connecting the three buildings and built on single mode optical fibre, was working on a speed of 200 mbps and had tremendous potential for upgradation to higher speeds including ATM. Further, RAILNET vulnerability could be compensated by having in place a combination of good configured firewall and intrusion detection system. It was also noticed that even after a lapse of five years since installation, the utilisation of ROLIN was low and SR was making efforts to lease out extra bandwidth to non-railway users, wherever possible, as directed by Railway Board.

---

[3] megabits per second

[4] Financial Adviser and Chief Accounts Officer

1.5.4 Operation of excess manpower

SR had deployed Data Entry Operators (DEOs) and Senior DEOs for development, testing and implementation of AFRES and PRIME modules in addition to their regular data entry work. Since the DEOs had access to all the stages, the system was exposed to the risk of unauthorised transaction processing and subsequent removal of any trail, thereby creating a major control weakness. This was not in accordance with the commonly adopted practice of allowing users at various levels to have access rights and permission on 'need to know and need to do' basis only. Moreover, SR had incurred avoidable expenditure of Rs.2.41 crore from October 2001 to March 2005 for operating 53 posts, including DEOs, in excess of requirements.

SR contended that there was heavy pressure on the EDP Centre to implement PRIME and AFRES in all Depots, workshops and divisional offices in SR and the remaining modules are to be implemented and customised and therefore it was utilising the services of DEOs and Senior DEOs for development and implementation of the application also.

The reply, justifying the requirement of DEOs and senior DEOs, did not address the control weakness that was created by associating DEOs and Senior DEOs with development and implementation of the application simultaneously with data entry work.

SR also had not carried out a fresh study of manpower requirement after the implementation of PRIME and AFRES systems resulting in continued extra expenditure on account of excess operation of posts.

1.6 Deficient general controls

General controls create the environment in which the application systems and application controls operate e.g., IT policies, standards and guidelines pertaining to IT security and information protection.

Audit observed that there was no security policy prepared by the railway administrations. Access controls and change management controls were also deficient, rendering the system vulnerable to unauthorised access.

1.6.1 Deficient system security

The Information Systems security policy aims at protection of valuable assets including hardware, software and data against possible risks of unauthorised access and misuse. It also aims to prevent any possible damage by employing suitable logical and physical access controls and ensuring proper segregation of duties.

* In SR the security policy was not framed and circulated among PRIME users. Moreover proper password controls were not established. Common passwords were assigned for a group and log-on identification (ID) was also being used as password for access, thereby rendering the system vulnerable to unauthorised access.

SR replied that username and password were very confidential and were changed frequently and that the supervisory staff in charge of the section was responsible for the confidentiality of the password. The reply was not tenable as the user ID and password should be confidential to the respective individual users and not to the supervisory staff and passwords should be unique to the users and not to a group.

* Similarly, in WR security policy was non-existent and proper password controls were not established. Log-on ID was being used as password for access. WR replied that individual passwords were issued to the employee responsible for the correctness of the pay sheet as well as data and a pay sheet clerk could neither see nor modify data of bill units allotted to another clerk**.** WR further stated that clerks were permitted to modify the master data since changes had to be recorded whenever an employee was promoted or transferred. However, as a rule for good system security, users should not have blanket access to master data. In exceptional cases this can be provided after proper authorisation and documentation, since it could affect the integrity of the database.

* For proper physical security the server as well as terminals used by the administrators should be physically separated from the other terminals. Disabling the floppy disk drive and CD-ROM[5] drive could control further access to data.

  In SR, in three locations, the servers as well as the operator terminals were in the same cabin, thereby impinging on access and physical security and the server and operator console were located in a physically unsecured area. All workstations in SR, which had access to the server, had floppy disk and CD-ROM drives. This security aspect was also not considered in WR.

* Organisational and management controls provide for proper and clearly defined levels of responsibility by adequate separation of duties within the information-processing environment. In SR and WR, edit and delete functions were possible at the same levels as data entry, even after the stage when data entry was complete and the record processed whereas this function should be vested only at higher supervisory levels.

  SR held that the staff at various levels was expected to function in a 'multi-skilling' mode and any rigid bureaucratic system would only hamper the on-going development and customisation of these packages to incorporate changes that occurred in the procedures. SR added that separation of data entry and edit/delete functions had to be viewed in the practical context considering the large number of staff and the

[5] Compact Disk Read Only Memory drives

amount of data modifications that were required. The master tables, however, could be modified only by the system administrator.

The practice of providing total access on the grounds of deploying staff in 'multi-skilling' mode was fraught with risks as it adversely affects the system integrity and creates a risk whereby the persons conducting the transactions can also erase the trails in case of irregular transactions. Segregation of duties in an operational system is one of the vital preventive controls to fix accountability and responsibility, considering that the application is processing transactions and is no longer in the test mode. This assumes importance as the system was found to be running with major deficiencies in validation controls and processing logic as detailed later.

1.6.2 Lack of change management control

All system changes should be authorised at appropriate levels, thoroughly tested, approved and documented. To control the on-going maintenance of the system a standard methodology for performing and recording the changes is necessary.

It was observed that no records were maintained in SR and WR to indicate the requests for change and the changes carried out in the system. In the absence of any evidence in support of the authorisation, modification carried out, testing and acceptance by the user, the changes made could not be subjected to verification.

SR, while stating that the software modules were undergoing a post-implementation phase of customization, held that detailed documentation would be impossible at this stage because of the dynamic nature of changes taking place and that only authorised staff and officers had access to the back-end and the source code. Procedures would have to be thought out after the whole system had stabilized and the users themselves were fully conversant with the core of the software.

The reply of SR cannot be accepted as, in the absence of documentation, running of the system becomes dependent on a small group of persons, which is not conducive either to transparency or sustainability of systems. Moreover formalizing change management controls was imperative to ensure that changes in the system were carried out only through formal requests from the authorised functionaries capable of being tracked and monitored at appropriate levels. Not documenting the changes creates an unacceptable risk towards the business continuity in case of a disaster, as there would be no frame of reference with which to compare the recovered functions.

WR contended that the vendor carried out the modifications only after authorisation at higher level. However, Audit noted that proper documentation was still a necessity in the interest of good change management controls.

1.6.3 Absence of disaster management and business continuity plan

The existence of a well-laid out recovery and reconstruction plan is essential in a computerised environment to revive operations expeditiously and

effectively. To ensure that the activities of information systems operations and its supportive role are not interrupted in the event of a disaster, secondary storage media such as tape reels, tape cartridges, removable hard disks or cassettes are used to store programs and associated data for backup processes. These secondary storage media are stored in one or more physical facilities - referred to as offsite libraries - based on availability of use and perceived interruption risk and also to ensure the presence, synchronization and currency of critical media and documentation. Offsite storage facility should be located away from the building housing the primary information processing facility.

In SR, backups (including data files, application software, application documentation, system software, system documentation, operation documentation) were stored in the same building housing the primary information processing facility. In the absence of offsite storage facility, it would not be possible to recover and continue the Information Systems (IS) operations and its supportive role in the event of disaster. SR contended that the database of Chennai Division and Headquarters was backed up and stored in a separate building. The reply is not acceptable because the offsite libraries are presently located at places which are not far away from the primary information processing facility and could also be subject to the same natural disasters (floods, earthquakes etc).

In WR, there was no laid down policy for disaster management and business continuity plan. Further there was no documentation specifying procedure, periodicity and personnel responsible for taking backup of data and application. Moreover, there was no record of testing done periodically for restoration of data from the backup. WR stated that the database dump files were backed up twice on daily basis on online media on two different machines and offline media on two different Digital Audio Tapes in append mode, hence contingency check was performed on a daily basis. While backup of data was being taken, proper documentation and maintaining off site libraries was necessary in the interest of good change management and business continuity plan in case of any contingency.

1.6.4 Deficiencies in system administration

Efficient and effective utilization of a financial application depends on proper and timely data entry, updation and deletion of data in master files and other related files. Not doing so would limit the utility of application and result in manual intervention without proper validation leading to the risk of irregular payments.

In WR, it was observed that out of 6,384 records of employees in the master files, master data in respect of 1,254 retired employees was not deleted or transferred from the payroll master file to the pension master file. Also, data was not fully entered in 90 out of 109 fields in the main master file. Further, in a number of cases data in respect of 20 crucial fields, required for generation of correct payroll, was left blank.

While WR agreed to correct the past cases, a structured system needs to be put in place to ensure prompt updation of master files as soon as the change occurs.

1.7 Inadequate application controls and inconsistencies with extant rules and regulations

Application controls relate to the specific tasks performed by the system and comprise of input, processing and output controls. Application controls are designed to provide an assurance that all inputs are properly authorised and complete, validating checks are in place, processing was done as designed and outputs are accurate.

Substantive testing, using test data and analytical review of data disclosed that the application controls were weak and the software had inherent deficiencies, which not only made it possible to process irregular transactions related to pay, allowances, recoveries and advances but also made it difficult to fix accountability. This led to overpayments and short recoveries and the risks of reliance on the system were high.

1.7.1 Deficient audit trail and non involvement of internal audit in system development

Audit trails are an essential component of all well-designed systems. They assist the Information Systems department as well as the Information Systems auditor by providing a map for retracing the flow of a transaction and enable the user and auditor to recreate the actual transaction flow from its origin to its existence on an updated file.

It was observed that the audit trail feature was disabled in SR and WR. It was also seen that in SR, the Internal Audit section was not involved in the system development and due to which, audit requirements were also not taken care of by the system. Information systems were not included in internal audit inspection schedule.

SR contended that it was premature to talk about audit trail in a dynamic situation where the stabilisation was yet to be achieved. Further, Headquarters personnel branch had a full fledged audit trail set up, which was tested and could be incorporated at any point of time, depending on the need as decided by the administrator. SR however accepted that inspection schedules for internal audit so far included the checks enumerated in the Inspection Manual and the system check, if necessary, could be done once in two years by duly incorporating this schedule like other Headquarters offices.

The reply was not tenable as the system was four years old and the audit trail was yet to be enabled. Audit trail and log files of all significant activities should have been incorporated in the system, which is already operational and processing live transactions. Involvement of internal audit in system development would have acted as a control against the application software deficiencies resulting from non-incorporation of validation checks in the system.

1.7.2 Deficient validation check for basic pay

Basic pay in the railways is normally within a predetermined range i.e., pay scale. The application should have inbuilt validation checks to allow pay within the prescribed pay scale only. Further, it should not allow a different pay scale to a person belonging to predefined scale or group.

Test check using dummy data in SR and WR disclosed that it was possible to input data under basic pay which exceeded the maximum of the scale. For example the system accepted basic pay of Rs.9,525 in the scale of Rs.5,500-9,000 and Rs.20,000 in a pay scale of Rs.7,450-11,500 in SR and WR respectively, indicating lack of validation checks.

The contention of SR that the option of paying more than the maximum of the scale was left open to enable higher pay after allowing stagnation increment was not acceptable since such option should only be enabled on a case to case basis or alternatively a separate column for stagnation increment could be created rather than enabling it across the board.

In SER, the system accepted a lower scale of pay for higher designation. For example a Group 'D' pay scale of 2,550-3,200 was accepted for the Deputy. CAO, who is a Group 'A' officer. Conversely a higher scale of pay was accepted for a lower designation e.g. Group 'C' pay scale of Rs.5,500-9,000 for a van cleaner, which is a Group D post. The system also accepted any 'Group Code' for any 'Designation Code' of an employee; for instance a Group 'C' code for FA&CAO, a Group 'A' officer. The reply of SER that it was still depending on manual checks confirms that the computerised system was unreliable.

1.7.3 Poor validation control for allowances

The railways grant various allowances such as Transport Allowance, Dearness Allowance, Running Allowance, Non-Practicing Allowance, Nursing Allowance etc., to employees. Review and substantive testing using dummy data revealed that the validation mechanism was poor leading to acceptance of irregular transactions and overpayments.

Transport Allowance

Extant orders envisage that an employee could avail of either the facility of transport allowance or that of Residential Card (RC) pass. In SR, a check using dummy data disclosed that the system accepted Transport Allowance of Rs.100 even though the RC pass field was marked as "Y" indicating that the facility of RC pass was being availed. Data analysis of 120 cases revealed that in the absence of proper indication in the master data, in five cases Transport Allowance was paid while RC pass was being availed.

SR, while mentioning that the overpayment has since been recovered from four employees, stated that information regarding the staff availing RC pass was not designed for validation for Transport Allowance. Further, the practice of allowing both RC pass and half the entitlement of conveyance allowance for physically handicapped persons required flexibility in such validation. The

contention was not acceptable. SR should establish correlation between the fields of RC pass, physically handicapped employees and Transport Allowance in the system for better control over Transport Allowance without any manual intervention.

Similarly in WR, the system allowed a dummy data of Rs.400 as Transport Allowance when both RC Pass and Office Transport fields were check marked to indicate that both the facilities were being availed.

Data analysis in SER also revealed that Transport Allowance was paid to the staff irrespective of the station code, which resulted in an excess payment to four employees. Moreover, Transport Allowance was also drawn in case of 21 employees, where no station code/ locality code was assigned in the database.

The reply of SER that Transport Allowance was drawn basing the locality code as A1 is not acceptable, as there was no entry against locality code in the data provided.

Dearness Allowance

Rates of Dearness Allowance are enhanced from time to time by Government of India notifications. The Dearness Allowance was enhanced by two per cent and by three per cent with effect from January 2004 and July 2004 respectively. Accordingly, arrears of Dearness Allowance were to be calculated by the system for the periods for which it was not drawn through regular salary bill.

Analysis of data in SER for the months of March 2004 and October 2004 revealed that system accepted invalid period for calculation of arrears of Dearness Allowance (shown as commencing from December 2003 and June 2004 respectively) during input and hence excess arrears of Dearness Allowance were paid to staff.

While SER accepted the finding and assured recovery of the amount overpaid, proper input validation controls need to be established in the system to ensure that invalid input is not accepted.

Other Allowances

The validation checks in respect of various other allowances were also found to be weak as follows.

- Though Over Time Allowance (OTA) was not admissible to staff except for Staff Car Drivers, operational staff and industrial employees, in SR, the system accepted OTA for non-entitled staff. Similarly in WR, the system accepted a dummy data of Rs.10,000 as OTA for a group 'B' officer.
- Washing Allowance is only admissible to a designated category of staff. However, in WR, the system accepted dummy data of Rs.500 as Washing Allowance for an ineligible officer. Similarly in SER, Washing Allowance of Rs.30 was allowed to FA&CAO, a Group 'A' officer in the pay scale of Rs.18,400 –22,400. SER conceded that validation was not feasible and manual checks had to be maintained.

Audit noted that the system required immediate correction to incorporate the necessary validation.

* As per rules, Non Practising Allowance (NPA) is admissible only to doctors. However in WR, the system allowed NPA to staff other than doctors when the NPA code was entered in the system.

* In WR, the system allowed House Rent Allowance (HRA) to even those staff provided with residential quarters. The system also allowed HRA to an employee when a dummy amount of Rs.5,000 was entered as rent recovery.

* In SER, the system accepted Nursing Allowance to employees other than nursing staff. For example, Nursing Allowance of Rs.1,600 was allowed to Deputy FA & CAO. SER stated that validation was not feasible and manual checks had to be maintained.

* As per rules the rates of National Holiday Allowance (NHA) varied with the pay of the employee. Owing to non-incorporation of the prescribed rates, in SER, the system accepted any amount entered as NHA irrespective of rate of pay. For instance Rs.106 was accepted as NHA as against an admissible amount of Rs.140 for pay of Rs.9,475. SER agreed to incorporate the rates of NHA in the program.

1.7.4 Recoveries

Audit observed that the validation controls provided in the system for effecting recoveries were inadequate resulting in improper recoveries. This also adversely affected the integrity of the system.

* In WR and SER, the system was accepting any amount as VPF, in excess of monthly pay in contravention of provisions of the Indian Railway Establishment Code. In SR, the amount of subscription towards State Railway Provident Fund was recovered less than the stipulated $8^{1}/_{3}$ per cent of pay in some cases and in others the subscription to Provident Fund including VPF exceeded the pay drawn for the month. SR has now rectified the error pointed out. However, rectifications in WR and SER were yet to be carried out.

* In SER, the system accepted the dummy data of Rs.30 per month as subscription to Group Insurance Scheme for a Group 'A' officer, instead of the mandatory Rs.120 per month. In SR, subscription to Railway Employees Group Insurance Scheme amounting to Rs.0.63 lakh, pertaining to 232 cases in Workshop, Perambur and 3,018 cases in Tiruchirapalli and Trivandrum divisions was not recovered. The cases pertained to existing employees already covered under the scheme and who were on leave without pay and from whom no recoveries were made after their resuming duty. SR stated that further details were required and facts regarding non-recovery were to be ascertained and that recoveries could be done only from the next calendar year in respect of new employees and absentees.

* Profession Tax is deductible at prescribed rates on the gross emoluments drawn by the employee and the drawing and disbursing authority is liable to remit exact amount to the respective State Government. In SER, the system accepted any rate of Profession Tax without any correlation to the prescribed rates applicable in the State in which an employee was posted. For instance, the levy of Profession Tax at a rate applicable to West Bengal was accepted for employees posted at Visakhapatnam and Bilaspur. The system also accepted incorrect rates. For instance, in the case of an employee of West Bengal drawing a gross pay of Rs.32,750 the system accepted Profession tax as Rs.130 instead of Rs.150. Analysis of data files in SER, for the period from April 2003 to April 2004 and July 2004 to May 2005 revealed that revised rate of Profession Tax with effect from 1 April 2003 were not incorporated in the system resulting in short recovery of Profession Tax from members of staff.

  SER stated that validation on station could not be enforced as in many cases station code is 'NULL'. This indicates that though IT enabled business solutions were undertaken, adequate process re-engineering was not done and all material information about the employees, required as inputs into its system was not being collected. Prescribed rates were also not being updated in the system.

  In SR, non-recovery and short recovery of Profession Tax and other dues such as quarter rent and electricity charges to the extent of Rs.0.13 crore was noticed. SR stated that rent and water charges have since been recovered. As for Profession Tax, information about the period of recovery and the other modalities were being clarified.

* The recovery towards Compulsory Monthly Thrift Deposit at the rates prescribed by South Eastern Railway Employees Co-operative Credit Society Ltd., Garden Reach, Kolkata was to be effected, as advised from time to time from the salary of the employees on the basis of their pay. In the absence of incorporation of prescribed rates in the system and lack of validation control, Compulsory Monthly Thrift Deposit was recovered as entered by the bill-preparing unit irrespective of the pay of the employee and the system failed to detect the incorrect recovery. Analysis of data revealed a short recovery of Compulsory Monthly Thrift Deposit amounting to Rs.0.04 crore during April 2004 and from July 2004 to May 2005. SER agreed to carry out necessary corrections in the program. Railways need to ensure incorporation of prescribed rates and validation controls in the system.

1.7.5 Advances

Railways sanction various advances like Festival Advance, Cycle Advance, Fan Advance etc. to employees depending on their cadre and their scales of pay. Review of various advances sanctioned through PRIME disclosed poor input validation controls over sanction and calculation of advances.

* Rules provide for the grant of an interest free Festival Advance of Rs.1,500 on one occasion in a calendar year only to non-gazetted Railway employees whose basic pay did not exceed Rs.8,300 per month. However, in SR and WR, the system allowed an amount of Festival Advance not only beyond the permissible limit of Rs.1,500 but also to non-eligible staff. For instance the system accepted a dummy data of Rs.2,000/ Rs.3,000 as grant of Festival Advance for a Group 'B' officer. Further, in SER, an amount of installment of Festival Advance was allowed as recovery from the salary of Deputy Chief Accounts Officer (Group-A officer) for five different festivals simultaneously. The reply of SER that this validation was done manually since the feeding form was common for all advances is not tenable because proper validation had to be built in the system itself. Further, test check of Headquarters payroll of 2004-05 revealed that in eight records the festival advance was granted even though basic pay had exceeded Rs.8,300 per month.

* In SER**,** the system allowed recovery of Cycle Advance from the salary of Group A and B officers though the Cycle Advance was admissible to only non-gazetted employees whose basic pay does not exceed Rs.5,000 per month.

* In SER, the system allowed recovery of Motor Car Advance from the salary of Group 'D' staff whose maximum scale of pay was Rs.3,200 per month though only officers having a basic pay of Rs.10,500 or more were entitled to Motor Car Advance.

* In SER, the system allowed recovery of Fan Advance from the staff other than Group 'D' staff also (viz., Senior Section Officer) though only Group 'D' staff were entitled to Fan Advance. SER agreed to make necessary modifications including incorporation of validation checks into the system.

1.7.6 Other Irregularities

* In case of 98 members of staff, in SER, the date of birth field in the database was left blank though their salary was being drawn on a regular basis. Data analysis of pay roll master and transaction files of headquarters and various divisions for the period 2002-03 in SR, also disclosed that vital data such as date of birth, date of joining in the service, scale code, group insurance category, city classification, RC pass indication etc were left blank. In the absence of specific indication in these fields, the correctness of pay and allowance did not lend itself to verification. SER accepted the deficiency and assured requisite rectification.

* In WR, the system generated salary bill for October 2005 even when a dummy date of birth was entered as 29 March 1930 indicating the age of employee as over 75 years whereas the normal age of retirement in Indian Railways is 60 years. In SER, the system allowed drawal of pay and allowances for the month of August 2004 for an employee, whose

date of retirement was 31 May 2004. Further, when a dummy date of birth was entered as 31.12.1944, the date of retirement was incorrectly generated by the system as 31.12.2104 instead of as 31.12.2004. Analysis of data of employee master file for April 2004 in SER, revealed that the system had calculated a wrong date of retirement in 25 cases taking the length of service ranging from 61 years to 1,061 years, which clearly illustrated erroneous processing. SER replied that the validation check was disabled and that unless and until the date of birth of all employees was filled with authenticity, no control could be incorporated in the program. This indicated that the available data was incomplete and raised serious questions about the reliability of the system.

1.8 Recommendations

* Railways need to draw up a full fledged IT policy, implementation plan, adequate documentation and security policy in respect of application systems and physical storage of data.
* Railways need to strengthen the standards of IT control such as segregation of duties, logical access controls and change management control.
* Railway administration should bring out a proper plan including fixation of a suitable target date so that PRIME can be implemented with proper validation checks in a properly controlled environment.
* The application PRIME should be modified and upgraded to include additional data validations in order to eliminate the drawbacks pointed out in the system.

1.9 Conclusion

Though PRIME met the Railway's objectives partially, the application did not conform to normal standards of good IT practices. The application software has been developed without taking into account important conditions governing the calculations of pay, allowances, advances etc. Controls to ensure transparency and integrity of the database are also lacking in the system. Since the system is run in a poorly controlled environment with inadequate documentation and has major deficiencies regarding restricting the processing of pay, allowances, advances and recoveries in consonance with relevant rules, the risk of reliance upon the system in its present form was high. Absence of proper security policy and access control mechanisms coupled with absence of audit trail makes the system vulnerable to manipulation.