

00307



सत्यमेव जयते

Report of the
Comptroller and Auditor
General of India

for the year ended March 2007

Union Government (Railways)
No.PA 18 of 2008
(Information Technology Audit)

©

**COMPTROLLER AND AUDITOR
GENERAL OF INDIA**

2008

Website: <http://www.cag.gov.in/>

PRICE

INLAND : Rs 65.00

FOREIGN : US \$ 5

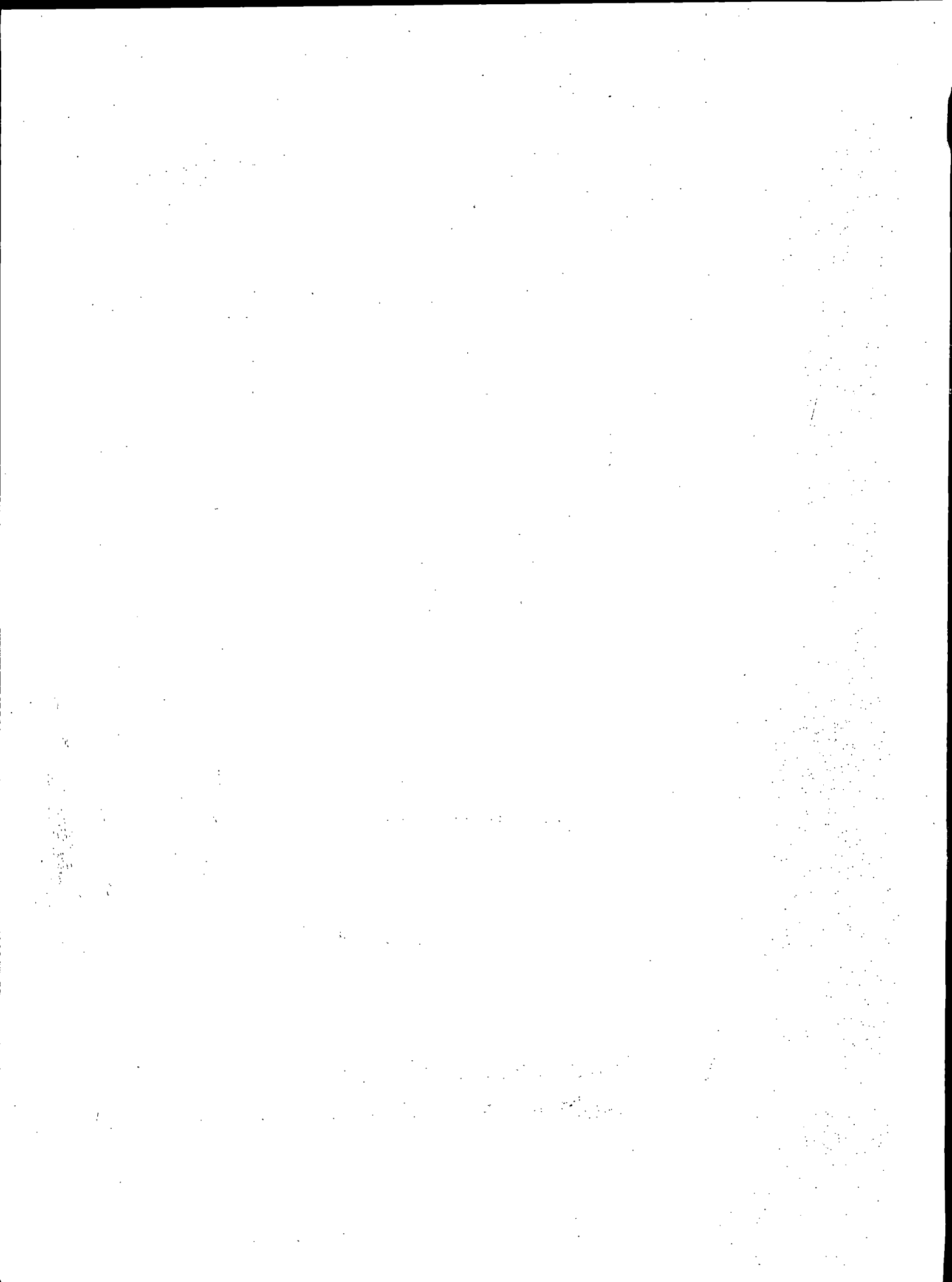
(Including Postage/ Air Mail)

**Report of the
Comptroller and Auditor General
of India**

for the year ended March 2007

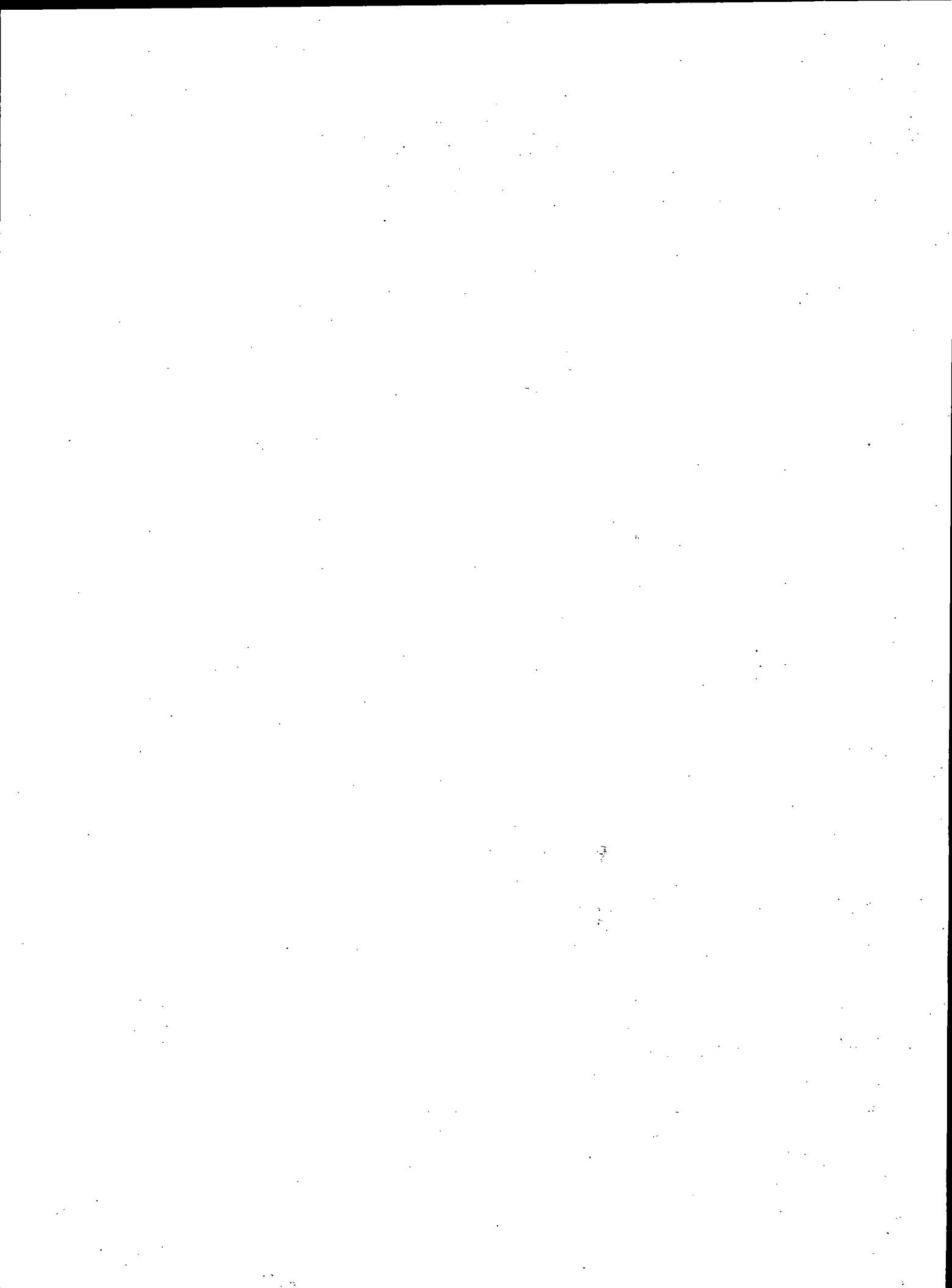
Laid in Lok Sabha/ Rajya Sabha on _____

Union Government (Railways)
No. PA 18 of 2008



CONTENTS

	Paragraph	Pages
PREFACE		ii
OVERVIEW		iv-v
CHAPTER 1 – UNRESERVED TICKETING SYSTEM IN INDIAN RAILWAYS		
Highlights	1.1	1
Gist of recommendations	1.2	2
Introduction	1.3	3
Organisation	1.4	3
Audit objectives	1.5	4
Audit scope, criteria and methodology	1.6	4
Audit findings	1.7	4
Acquisition and implementation	1.8	5
General controls	1.9	12
Application controls	1.10	18
Conclusion	1.11	24
CHAPTER 2 – OTHER COMPUTERISED APPLICATION IN INDIAN RAILWAYS		
IT Security on Western Railway	2.1	25
Highlights	2.1.1	25
Recommendations	2.1.2	25
Introduction	2.1.3	25
Audit objective	2.1.4	26
Audit scope, criteria and methodology	2.1.5	26
Audit findings	2.1.6	26
Conclusion	2.1.7	31
Provident Fund Accounting System in Izatnagar Division of North Eastern Railway	2.2	31
Highlights	2.2.1	31
Recommendations	2.2.2	32
Introduction	2.2.3	32
Audit objectives	2.2.4	32
Audit scope, criteria and methodology	2.2.5	32
Audit findings	2.2.6	32
Conclusion	2.4.7	35



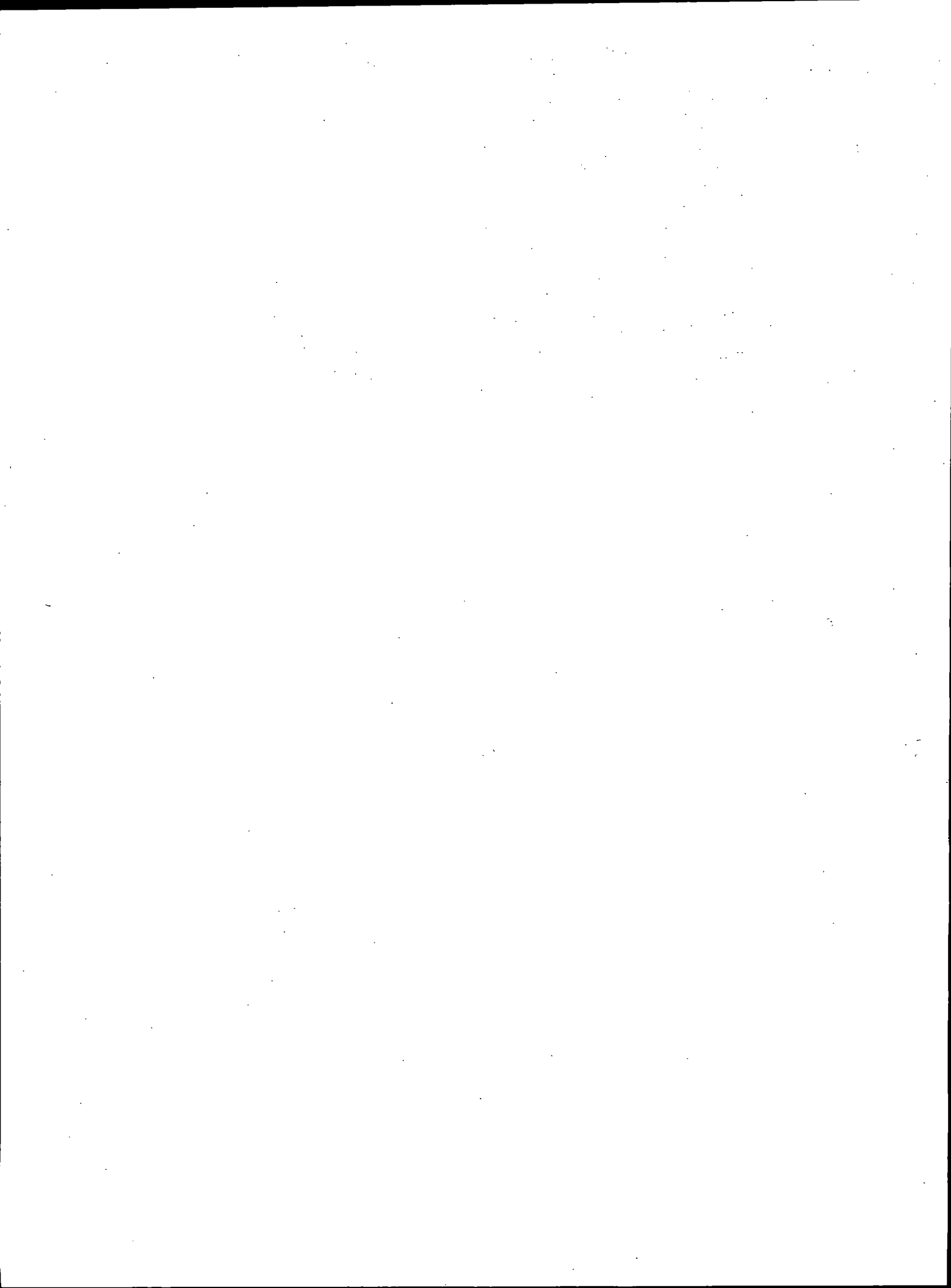
PREFACE

The benefits of computerisation have been extensively exploited in Indian Railways. Some applications have been developed as standardised applications for implementation across Indian Railways. Zones have also been developing several applications locally to manage various functions. Information Technology (IT) audit of some applications were carried out using Computer Assisted Audit Techniques (CAATs) to verify the integrity, completeness and availability of data and the findings are included in this report.

This report is divided into two chapters:

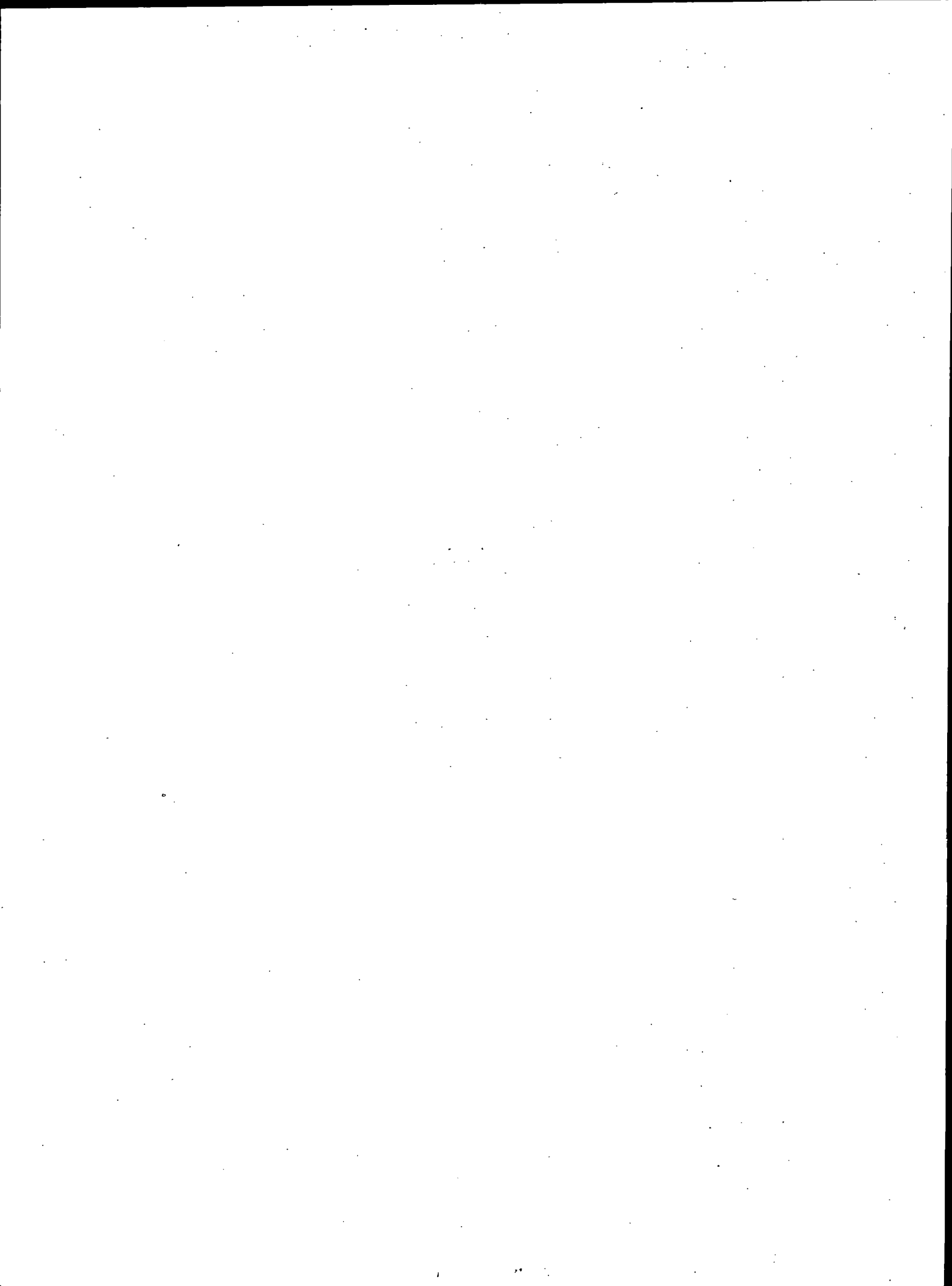
Chapter 1: Contains the findings of the IT audit of the Unreserved Ticketing System (UTS), a computerised application that has facilitated purchase of unreserved tickets three days in advance of the date of journey from the UTS counter for all such destinations which are served by that station and has simplified the process of cancellation of unreserved tickets. The application was audited across all zones of Indian Railways.

Chapter 2: Contains findings of the IT security audit of the computerised applications in Western Railways and the audit of Provident Fund Accounting system in Izatnagar Division of North Eastern Railway.



Abbreviations used in the Report

CR	Central Railway
ER	Eastern Railway
ECR	East Central Railway
ECoR	East Coast Railway
NR	Northern Railway
NCR	North Central Railway
NER	North Eastern Railway
NFR	Northeast Frontier Railway
NWR	North Western Railway
SR	Southern Railway
SCR	South Central Railway
SER	South Eastern Railway
SECR	South East Central Railway
SWR	South Western Railway
WR	Western Railway
WCR	West Central Railway



OVERVIEW

Chapter 1 Unreserved Ticketing System in Indian Railways: Unreserved Ticketing System provides the facility to purchase unreserved tickets three days in advance of the date of journey and has simplified the process of cancellation of unreserved tickets. Indian Railways planned implementation of Unreserved Ticketing System initially at 23 locations in Delhi area. Centre for Railway Information System (CRIS) was the nodal agency for procurement of hardware and development of software, which commenced in August 2002. Unreserved Ticketing System has since been replicated in all the zones of Indian Railways.

The Information Technology audit of Unreserved Ticketing System (UTS) over various zones of Indian Railways disclosed several deficiencies. The decision to procure dot matrix printers for initial phases of implementation of UTS at different locations despite knowing its vulnerability to manipulation rendered the system prone to misuse and frauds (Para 1.8.1). Even though the UTS services were frequently disrupted by extensive link failures in the leased communication channels provided by BSNL/MTNL, there was no mechanism to ensure minimum guaranteed efficiency of the leased lines. The plan to provide thin clients in smaller stations experiencing frequent link failures was not achieved even after a lapse of about five years (Para No 1.8.2). The system was not comprehensively designed and had various deficiencies, which not only caused operational constraints but also warranted manual intervention leading to increased security risks and inconvenience to passengers (Para No 1.8.3). Disaster recovery and business continuity plans were not formulated and the back up measures were not tested leading to operational problems. Inadequate physical and logical access controls exposed the system to unauthorised access and IT assets were not adequately protected. Change management controls were also weak (Paras 1.9.1 to 1.9.3). Validation controls for cancellation of tickets and issue of both advance journey tickets and season tickets were inadequate. The policy of allowing cancellation of non-suburban tickets was prone to misuse in case of travel to short distance destinations. Fares and distances between stations were incorrectly adopted in the system leading to incorrect levy of fares from passengers. Several routes were not defined in the system preventing issue of tickets to destinations. The database contained various inaccuracies casting doubts on its reliability (Paras 1.10.1 to 1.10.4). The system was also deficient in controls to monitor and check any fraudulent use of pre printed ticket stationery (Para 1.10.5).

Chapter 2 Other computerised applications in Indian Railways: Information Technology Security of the computerised applications in Western Railway suffered from various deficiencies such as lack of IT security policy and failure to conduct any threat based risk assessment for systems and data. An independent vulnerability assessment revealed as many as 274 vulnerabilities out of which 197 were of high risk. Network security was inadequate as open ports were found in personal computers rendering the systems vulnerable to viruses, worms and intrusion by hackers. Both the physical and logical access controls were inadequate exposing the systems to

unauthorised access and malicious software (**Paras 2.1.6.1 to 2.1.6.3**). Physical and information assets in Western Railway were not classified and there was no mechanism to designate ownership of critical information. Training in IT security was inadequate and internal audits of IT assets, application and its security were not conducted (**Paras 2.1.6.4, 2.1.6.6 and 2.1.6.7**).

The Provident Fund Accounting System in Izatnagar Division of North Eastern Railway suffered from defects such as business rules relating to accounting of Provident Fund transactions not being incorporated leading to incorrect processing of transactions, inadequate validation controls which adversely affected the reliability of data, weak access control mechanism and absence of audit trail rendering the system vulnerable to manipulation. The system was not functioning concurrently with the Pay Roll System and therefore up to date balances of subscribers' Provident Fund accounts were not available (**Paras 2.2.6.1 to 2.2.6.4**).

Chapter 1 Unreserved Ticketing System in Indian Railways

1.1 Highlights

- Indian Railways did not have any structured mechanism for resolving delays on the part of CRIS in acquisition of hardware and peripheral equipments. The decision of Indian Railways to procure dot matrix printers for initial phases of implementation of UTS at different locations despite knowing its vulnerability to manipulation rendered the system prone to misuse and frauds.

(Para No 1.8.1)

- The Unreserved Ticketing System was frequently disrupted by extensive link failures in the leased communication channels provided by BSNL/MTNL and Indian Railways did not have any mechanism to ensure minimum guaranteed efficiency of the leased lines. Indian Railway's plan of providing thin clients in smaller stations experiencing frequent link failures was not achieved even after a lapse of about five years.

(Para No 1.8.2)

- The system design did not comprehensively incorporate all the business rules and had various deficiencies, which not only caused operational constraints but also warranted manual intervention leading to increased security risks and inconvenience to passengers.

(Para No 1.8.3)

- Disaster recovery and business continuity plans were not formulated and the back up measures were not tested leading to operational problems.

Para No 1.9.1)

- Inadequate physical and logical access controls exposed the system to unauthorised access and IT assets were not adequately protected. Change management controls were also weak as changes were carried out incorrectly or belatedly after revision of rules. Changes were not documented.

(Para Nos 1.9.2 and 1.9.3)

- Validation controls for issue of advance journey tickets, cancellation of tickets and issue of season tickets were inadequate. The policy of allowing cancellation of non-suburban tickets was prone to misuse in case of travel to short distance destinations.

(Para No 1.10.1)

- Fares and distances between stations were incorrectly adopted in the system leading to incorrect levy of fares from passengers. Several routes were not defined in the system preventing issue of tickets to

destinations; the validation controls for issue of blank paper tickets were also inadequate. The database contained various inaccuracies casting doubts on its reliability.

(Para Nos 1.10.2 to 1.10.4)

- The system was also deficient in controls to monitor and check any fraudulent use of pre printed ticket stationery.

(Para No 1.10.5)

1.2 Gist of recommendations

- Indian Railways may institute a structured mechanism incorporating penal provisions for deficiencies in performance vis-a-vis CRIS. The dot matrix printers should be replaced on priority with thermal printers to prevent the possibilities of misuse and to enhance the printing speed of tickets.
- Indian Railways should formalise service level agreements with BSNL/MTNL for minimum guaranteed efficiency of leased lines and penalties for link failures. Indian Railways should expedite replacement of dumb terminals with thin clients in a specified time frame to improve the continuity of UTS operations.
- The system should be comprehensively designed incorporating all the business rules relating to issue of unreserved tickets, to minimise manual interventions and to generate periodical reports accurately to enhance its utility.
- Indian Railways should have a documented disaster recovery and business continuity plan encompassing all factors relating to IT risks. The back up measures need to be tested on a regular basis to avoid problems of synchronisation.
- Indian Railways should develop a comprehensive IT policy. Adequate physical access controls should be instituted to safeguard UTS assets and access controls should be strengthened to ensure accountability for transactions. Assignment of various privileges should be standardised and adequate controls need to be established to prevent misuse of privileges.
- Indian Railways should institute a mechanism for effecting changes to the program logic promptly and accurately as and when revisions in the business rules take place. All changes should be properly authenticated and documented.
- Indian Railways should rectify the system and strengthen validation controls. Indian Railways may review its policy on cancellation of tickets issued for short destination journeys to prevent misuse. The fares and distances adopted in the system should also be rectified to be in accordance with the business rules and to ensure correct levy of fares from passengers.
- Indian Railways should assess the completeness of master data on priority and incorporate all routes in the database. The inaccuracies in the database

should also be rectified to enhance reliability of data. The control mechanism for issue of blank paper tickets may also be strengthened.

- Indian Railways may strengthen its monitoring mechanism for use of the pre-printed ticket stationery. Validation checks may be built in the system to highlight cases of discontinuity in ticket rolls.

1.3 Introduction

Indian Railways (IR) carries about 1.4 crore passengers everyday out of which about 1.2 crore passengers travel in unreserved coaches and thus form the bulk of rail users contributing significantly towards railway's earnings. A railway ticketing system software namely Scalable Modular Advanced Rail Ticketing System (SMARTS) was implemented (1998) over IR on stand alone Self Printing Ticketing Machines (SPTMs) for issuing unreserved tickets. While SMARTS contributed towards reducing ticket inventory and provided automated accounting at the station level, the system had several limitations viz., non-availability of the facility for across-the-counter cancellation of tickets, increased transportation cost in updating program logic, need for huge manpower and lack of centralised control over individual booking offices etc. To overcome these limitations, IR planned (2001-02) a new System - Unreserved Ticketing System (UTS) for implementation initially at 23 locations in Delhi area. Centre for Railway Information System (CRIS) was the nodal agency for procurement of hardware and development of software that started from August 2002. UTS has since been replicated in all the zones of Indian Railways.

UTS provides the facility to purchase unreserved tickets three days in advance of the date of journey. A passenger can buy a ticket for any destination from the UTS counter for all such destinations which are served by that station. The cancellation of tickets has also been simplified. Passengers can cancel their tickets upto one day in advance of the journey from any station provided with a UTS counter. On the day of journey, the ticket can be cancelled from any station of the cluster from where the journey was to commence.

UTS is developed on UNIX operating system with C++ language interface for the front-end and SYBASE for the backend database. UTS database is maintained on servers placed at seven locations across the country (Mumbai, Delhi, Kolkata, Chennai, Secunderabad, Gorakhpur and Patna).

1.4 Organisation

At the apex level, Railway Board is controlling the activities of UTS through the Computerisation and Information Systems Directorate. At the zonal level, UTS activities are controlled by Chief Commercial Manager who is assisted by Deputy Chief Commercial Manager, Senior Commercial Manager, Office Superintendents and other supporting staff. The technical support is provided by Deputy Chief Electrical Engineer, and Deputy Chief Signal & Telecommunication Engineer.

Development and maintenance activities of the UTS are managed by Center for Railway Information System (CRIS), which is headed by a Managing Director. The Managing Director is assisted by Group General Managers, Chief General Managers and General Managers. At the zonal level, CRIS is headed by Chief General Manager/General Manager who is assisted by Regional Manager/Managers and Senior Software Engineers/ Software Engineers.

1.5 Audit objectives

The review of Unreserved Ticketing System was conducted with a view to assess whether the:

- acquisition and maintenance of hardware, communication network channels and software including system design were adequate and effective.
- general controls were adequate and system was operating in an adequately controlled environment.
- application controls were adequate and the system was in compliance with business rules and adequately secured from possibilities of fraud.

1.6 Audit scope, criteria and methodology

The scope of audit review included test check of records maintained in the office of the CCM of zonal railways and at CRIS offices relating to development of software, procurement of resources, and implementation of the UTS for evaluation of general and application controls operating in the IT Environment.

The rules and provisions contained in Indian Railway Commercial Manual Volume –I, Indian Railway Conference Association's Coaching Tariffs, Indian Railway Stores Codes, guidelines, instructions and orders issued by Railway Board from time to time, minutes of the meetings, procedures defined by Railway Administration and best practices prevalent in IT environment were used as audit criteria for assessing the performance of the system.

Relevant documents/records about implementation of UTS including records of selected 254 locations [CR:20, ER:20, ECoR:12, ECR:9, NCR:4, NER:10, NEFR:19, NWR:10, NR:20, SCR:30, SER:17, SECR:10, SR:20, SWR:20,WCR:13, and WR:20] were scrutinised. Simulation tests were conducted at CRIS and different UTS locations through test data. Output generated by the system at different locations on various Zonal Railways was also checked. Analysis of UTS data was done through Computer Assisted Audit Techniques (CAATs) to verify the integrity, completeness and availability of data.

1.7 Audit findings

The audit findings are given in the following three sections:

- Acquisition and implementation
- General controls
- Application controls

1.8 Acquisition and implementation

Acquisition and subsequent maintenance of hardware, including the communication network, is vital for implementing the computerised system in a specified time frame and for providing uninterrupted service. Further, for a system to be implemented effectively, it is imperative that the system is designed comprehensively incorporating all the relevant business rules and is compatible with all situations so as to be operationally convenient and to be utilised optimally. Audit observed deficiencies in the acquisition and maintenance of hardware, communication network and system design as brought out below:

1.8.1 Deficient acquisition and maintenance of hardware

Railway Board had laid down year wise targets for implementation of UTS in identified locations across all zones. The hardware and peripheral equipment required for UTS at the various locations were to be acquired by CRIS. Zones were required to enter into Annual Maintenance Contracts (AMCs) with the original equipment suppliers for maintenance of the hardware acquired by CRIS. Audit observed that:

- There were delays in implementation of UTS in 12 out of the 16 zones. In most of the zones the delays were on account of inordinate delays by CRIS in acquisition of hardware and as a consequence IR was running behind schedule in implementation of UTS as shown below. This also indicated that IR's monitoring mechanism was weak.

Zone	Target		Actual implementation	Number of locations not yet implemented	Reasons
	Number of locations	Period			
SR	71	2006-07	27	44	Delayed acquisition by CRIS.
ER	203	2006-07	7	196	Delayed acquisition by CRIS.
WR	116	2005-06	54	62	Delayed acquisition by CRIS.
SCR	91	2005-06	66	25	Delayed acquisition by CRIS.
CR	90	2006-07	25	65	Non-availability of hardware. Delayed acquisition by CRIS.
NWR	10	2004-05 and 2005-06	1	9*	Implementation in 9 locations delayed up to 9 months due to delayed procurement of hardware by CRIS.
ECoR	45	2004-05 to 2006-07	23	22	
NFR	33	2006-07	2	31	
WCR	25	2006-07	Nil	25	Work still in progress.
SER	76	2004-05 to 2006-07	41	35	
NR	25	2004-05	6	19	
NCR	35	2006-07	Nil	35	Delayed acquisition by CRIS. (Phase -II) For phase one also, no progress during 2004-05 and only four locations out of 18 were covered up to March 2007 due to delayed supply of equipment by CRIS.

- In ECR, UTS locations could not be commissioned because communication channels made available by BSNL could not be tested. Review of records of Dhanbad division revealed that nine channels provided by BSNL could not be tested for want of modems. These channels were only verified with local leads and were lying idle. BSNL had already informed that lease rentals for the channels would commence from the date of testing with local leads. Therefore, non-commissioning the locations not only delayed implementation of UTS in ECR but also resulted in avoidable payments to BSNL.
- Railway Board in its 'Action Plan for Unreserved Ticketing', had decided in September 2002 itself that thermal printers, which are tamper proof and could print tickets at higher speeds, should only be used in UTS rather than the conventional dot matrix printers, which were susceptible to misuse and frauds. Railway Board Vigilance also advised and intimidated all the zones about the possibility of frauds in issue of tickets in UTS as booking clerks could abort or tamper with the printing process of a dot matrix printer and use the blank/partially printed tickets for issuing higher value tickets and embezzle amounts collected by subsequently showing the higher value tickets as not printed. Further, to check the genuineness of tickets, UTS project envisages provision of Hand Held Terminals (HHTs) to the Travelling Ticket Examiners. The HHTs would verify the bar code that would be printed on the ticket issued through UTS by comparing it with the number stored in the server. A legible bar code could be printed only through a thermal printer.

Despite the known vulnerability of manipulation with dot matrix printers by the booking clerks and inherent advantages of having thermal printers, IR proceeded with bulk purchases of dot matrix printers across all zones. For three zones alone, 1,296 printers were procured at a cost of Rs.1.32 crore (WR-400 printers costing Rs.0.48 crore, CR-298 printers costing Rs.0.27 crore and SCR-598 printers costing Rs.0.57 crore) rendering them susceptible to misuse and frauds. Further, the dot matrix printers deployed in the suburban stations in CR also led to formation of long queues in front of booking counters due to the slow printing speed of the printers.

Instances of manipulation of tickets generated through UTS were already noticed in ECR, NR and WCR. In ECR, unreserved tickets of low value were manipulated and converted into high value tickets and such manipulated tickets were used for travel as well as for seeking refunds thereby resulting in loss to IR. In NR, fraudulent practices were prevalent at a number of UTS locations such as Azadpur, Sonapat and Lucknow bypassing the security features of printers. Test check by audit at some UTS locations further disclosed that the security locks of four out of eight ticket printers at Lucknow, all the six printers at Haridwar and one out of the ten printers at New Delhi were unlocked. Keys were found with the operators at Lucknow and Haridwar. In WCR, platform ticket valuing three rupees generated by the system was manipulated by typing the destination as Surat and fare as Rs.209.

- Procurement of 866 thermal printers for the subsequent phases of implementation of UTS in WR and CR was entrusted to CRIS (474 printers for WR and 392 for CR). CRIS was, however, yet to acquire these printers adversely affecting the efficiency of UTS.
- The Memoranda of Understanding (MoUs) entered into by the various zones with CRIS did not provide for penal clauses and therefore IR did not have any mechanism to hold CRIS accountable for the delays in acquisition of hardware.
- A test check disclosed that AMC's for maintenance of computer hardware and peripheral equipment at UTS locations were not entered into by four zones (CR, NER, WCR and ECoR). In WR, though the AMC expired in September 2006, neither was it renewed nor was a fresh AMC entered into. In CR, AMC was not entered into for the networking equipment also, even though its warranty period had expired in October 2006. Further in CR, the faulty dumb terminals of various stations from all over the zone were transported to headquarters for service and maintenance.
- Even the basic equipment such as Uninterrupted Power Supply (UPS) to protect the equipment from power surges and to avoid power interruptions was not available in many locations in ER and ECoR. In SCR, the UPS provided was not working in many locations.
- After implementation of UTS, the self printing ticketing machines (SPTMs) were lying un-utilised in zones. In ER, 209 SPTMs withdrawn from service from 49 locations were lying un-utilised. In NCR also, SPTMs were lying un-utilised in 17 locations.
- Railway Board had decided (August 2004) that UTS being a critical passenger interface application, 25 per cent spares should be built up at each location. However, such spares were built up in only one station out of 20 stations test checked in WR.

Thus, the entire mechanism of acquisition of hardware and peripheral equipments was defective. While the procurement by CRIS was predominantly characterised by delays, IR's decision to procure dot matrix printers for the initial phase of implementation of UTS at different locations despite knowing its vulnerability to manipulation lacked logic. Further, IR did not have any structured redressal mechanism against CRIS for the persistent delays in acquisition of hardware. The maintenance of hardware and peripheral equipment was also poor.

Recommendations

IR may institute a structured redressal mechanism with CRIS by incorporating penal provisions for deficiencies in performance. IR needs to strengthen its monitoring mechanism to avoid slippages in achievement of targets.

IR should replace the dot matrix printers on priority with thermal printers to prevent the possibilities of misuse and fraud leading to leakage of revenue and to enhance the printing speed of tickets.

1.8.2 Deficient communication network

Data communication between locations and server was either through leased lines from BSNL or through Railway's own communication channels. Important locations had two channels; combination of BSNL and Railway channels while smaller locations had only one channel, either of BSNL or of Railways. Audit observed that:

- There were frequent and extensive link failures of BSNL channels in all the zones. Since UTS locations are provided with dumb terminals, which do not have a hard disk to store data, connection to the central database is lost in the event of communication link failures and tickets cannot be issued through UTS. The zone wise link failures, which adversely affected the availability of the UTS services are shown below.

Zone	Observations
NWR	Number of breakdown cases increased from 439 cases during 2005-06 to 676 failures during 2006-07, 83.14 per cent of the cases involving 1106.18 hours were due to link failures.
NEFR	The average hours lost in a month due to link failures ranged from 10 hours to 28 hours in various locations during the period from September 2006 to December 2006. Similarly during the period from January 2007 to March 2007 the downtime due to link failure ranged from 35 minutes to 56.18 hours in the two PRS cum UTS locations (Goalpara Town and Harishchandrapur).
NER	572.20 hours of downtime at various locations was attributed to link failures over a period of ten months from August 2006 to May 2007.
ECoR	In 10 out of 12 locations test checked, the daily average system down time ranged from 14 minutes (at Bhubaneswar) to 4 hours and 20 minutes (at CHE). Further, in Khurda Road Division, 90.1 per cent of the down time in May 2007 was due to link failures.
WR	In four locations viz; Vasai Road, Virar (suburban locations), Amalner and Nandurbar stations, the down time ranged from 3 hours and 12 minutes to 54 hours and 29 minutes in a month, which was mainly on account of link failures of BSNL/MTNL channels.
ECR	In Danapur Division alone, 229.12 hours were lost due to link failures during the period from 1 September 2006 to 10 October 2006.
WCR	At 13 locations test checked, 672 out of the 815 disruptions were on account of link failures and UTS terminals were out of service for 1694 hours and 7 minutes.
NCR	202 out of the 223 failure cases were due to link failures and the downtime ranged from five minutes to 5 hours and 45 minutes.
ER	In Howrah, 27 out of the 34 failures during October and November 2006 were due to link failures. The duration of failures ranged up to 21 hours and 25 minutes. Frequent link failures coupled with extensive power failures led to the closure of one UTS location at Pirpainti Station in Malda Division and tickets were being issued manually.
SER	Records relating to link failures were available only in nine locations out of 17 locations test checked and 233 failures were observed in these nine locations during the period from October 2005 to June 2007.

Chapter 1 Unreserved Ticketing System in Indian Railways

SECR	21 instances of system failures were reported at five locations during the period from January 2007 to March 2007 involving a total downtime of about 114 hours, which was mainly due to link failures.
SWR	There were frequent link failures ranging from 5 minutes to 8 days and printed card tickets/Blank paper tickets were issued in some of the stations during the link failures.
NR	596 cases of communication (including 17 dual channels) failures were reported during the period from March 2007 to May 2007.
CR	Major cause of failure of UTS was attributed to link failures. A review of failure register maintained at nine locations disclosed that the failure data in the database did not tally with the registers maintained by the locations, indicating that either all failures were not properly reported or they were not updated in the system.
SR	One instance of major communication failure occurred in December 2006 resulting in breakdown of UTS. The system was restored after a gap of 20 hours and during this period unreserved tickets were issued manually

- There was no service level agreement between the Railway administration and BSNL/MTNL explicitly setting out the minimum guaranteed efficiency and penalties for failure and IR continued to incur expenditure towards hire charges even though the leased communication channels were disrupted due to frequent link failures.
- As early as 2002, Railway Board decided to introduce thin clients, which have flash memory, at smaller stations where link failures are frequent so as to issue tickets through UTS even during link failures. After the link is restored these devices synchronise the transactions done during link failures with the servers to keep the database updated. The thin clients were to be procured by CRIS. Even though about five years has lapsed since Railway Board's decision, thin clients have not been provided in any UTS location over IR. Thin clients were not provided in various locations over ECoR, WR and NWR even though they were planned in 2004-05 and 2005-06. In SCR they were not provided even though Rs.16 lakh was already paid to CRIS for the procurement. While in CR 26 terminals of Mumbai suburban stations (Kurla, Ghatkopar and Thane) could not be commissioned for want of thin clients and thermal printers, in NER though 24 thin clients were purchased in May 2006 they were not yet installed at various locations by the engineers of CRIS.

Thus, even though communication link failures in the channels provided by BSNL/MTNL were extensive, IR did not have any mechanism to ensure minimum guaranteed efficiency of leased lines. IR's plan of providing thin clients in smaller stations experiencing frequent link failures has remained unachieved even after a lapse of about five years.

Recommendations

IR should formalise service level agreements with BSNL/MTNL for minimum guaranteed efficiency of leased lines and penalties for link failures. IR should expedite the replacement of dumb terminals with thin clients in a specified time frame to improve the continuity of UTS operations.

1.8.3 Deficiencies in system design

Audit observed several design deficiencies in the UTS software as indicated below:

- Concessions to be granted to various categories of passengers as per extant rules of IR were not defined in the system.
 - Provision to issue concessional tickets to members/students/industrial workers traveling in group, foreign students studying in India, persons attending annual sessions of all India bodies of educational, cultural and social importance and All India Women Conference, Teachers honoured with National Award by President of India on Teachers Day; were not made in the system. (ECR, NR, NEFR, ER and NWR).
 - In WR all the concession codes were not defined in the master database.
 - Concessions in some cases were improperly provided. In SECR, 50 per cent concession was improperly provided as against 30 per cent admissible as per rules for recipients of President's Police Medal for distinguished service.
- Even though issue of circular journey tickets was permissible as per IRCA coaching tariff there was no provision in the UTS software to issue circular journey tickets to passengers. (NWR, ECR, NR, CR, WCR, SWR, ECoR, ER, NER, WR and SR). Consequently passengers are being disallowed the benefit of lower rates for circular journeys apart from the inconvenience of booking tickets for each leg of the journey separately.
- As per extant rules, if a passenger misses the connecting train for his continued journey at any station owing to late running of the train in which he is travelling, the fare for the travelled portion would be retained and the balance fare for the un-travelled portion should be refunded within 3 hours of the actual arrival of the train. There was no such provision in the UTS software for cancellation of un-travelled portion of a ticket (ECR, NR, NWR, WR and SECR).
- The system does not provide for issuing a receipt for clerkage charge when unreserved tickets are cancelled. As such non accountal of the amount received towards clerkage charge was not ruled out as it was possible for booking clerks to collect the clerkage charge of Rs.10 while not actually cancelling the tickets and reissuing the same to other passengers. (ECoR, CR, ER, NER and SER).
- Unreserved tickets for various classes (Sleeper, Chair Car, AC III and First class) issued from UTS subsequently presented for reserved accommodation through Passenger Reservation System (PRS) could be cancelled through UTS only. UTS, however, did not have any provision for realisation of the cancellation charges as envisaged in the rules. These tickets were being cancelled manually, which was time consuming and inconvenient for passengers.

- UTS did not properly account for the cancellation of a ticket initially issued on 100 per cent concession vouchers such as military warrants etc. When such a ticket was cancelled, the system did not include the refunded amount through vouchers under 'voucher refunds' in the Daily train cash book-cum-summary (DTC) generated by the system at the end of the shift of the booking clerk resulting in an extra debit against the booking clerk. To regularise the transaction, a special credit was being obtained manually from the accounts department each time. (ECR, SR, CR, SCR, NER, NR, SECR and SWR).
- UTS was generating incorrect accounting reports. Many locations complained of discrepancy between the DTC and figures shown in the reports generated through UTS raising questions on the reliability of the information extracted from the system (SCR, ER, and NER). In SCR, the differences between DTC and cash reports range from Rs.3 to Rs.620. Though these differences are a recurring phenomenon in UTS, no action was initiated by CRIS to rectify the errors. A test check for the month of March 2007 in ER disclosed that transactions of seven days, as recorded in the Daily Summary of Transactions, did not tally with the corresponding figures in the Monthly Summary of Transaction (Cash Information). Such discrepancy was noticed in respect of both the servers, viz; Cal 1 and Cal 4. Likewise in NER, while the monthly statement for July 2006 for Pilibhit station indicated the figure as Rs.32,00,076 the corresponding 31 daily transaction summaries indicated the figure as Rs.32,62,126.
- Stock Roll Management Module, which facilitates users to enter the details of ticket rolls disbursements from stores and allows users to record the roll transfer from one booking location to another etc, was not implemented thereby rendering the system vulnerable to possibilities of frauds and manipulations in use of unaccounted tickets (NR, WCR, NWR, CR and ECoR).
- UTS also restricted the maximum number of passengers per ticket to four for second class /Mail express/ Ordinary, two for sleeper class and one for upper class (except AC I or AC II), which had the effect of inconveniencing the passengers.
- One of the objectives of UTS was to provide centralised accounting, database and system administration. UTS has not yet been integrated with Advanced Finance and Railway Earnings and Expenditure System (AFRES) or any other accounting system and therefore online information of UTS earnings or apportionment of UTS earnings over different zones could not be provided.

Further, as per the functional specifications, the system should generate Balance Sheet, Passenger Classification for the purpose of data for 6A Statement/Apportionment of Earnings and Cumulative Shortage-In-Booking (SIB)/ Excess-In-Booking (EIB). Audit scrutiny revealed that provision to generate these reports was not made in the UTS system. Presently monthly Balance Sheets of the stations are prepared on the daily

and monthly position of UTS earnings and other manual bookings. These are sent to Traffic Accounts Office for further compilation (ECR, CR, SER, SECR, WCR, WR, ECoR and NEFR).

Thus, the software had various deficiencies, which not only caused operational constraints and warranted manual interventions leading to increased security risks but also inconvenienced the passengers. The business rules relating to grant of concessions to various categories of passengers were not incorporated in the system.

Recommendations

The deficiencies in the system design pointed out above need to be rectified based on user requirements. The system should be comprehensively designed so as to encompass all the business rules of IR relating to issue of unreserved tickets, to minimise manual interventions and to generate periodical reports accurately to enhance its utility.

1.9 General controls

General controls regulate the environment in which the IT application is operated and includes disaster recovery and business continuity planning, access controls- both physical and logical access and organisational issues such as change management, segregation of duties and providing adequate training. Audit observed that the disaster recovery and business continuity arrangements were inadequate, IT security practices comprising physical and logical access and environmental controls were inadequate, change management was deficient and training of staff was inadequate as brought out below:

1.9.1 Inadequate disaster recovery and business continuity arrangement

A structured disaster recovery and business continuity plan is essential to reduce the risks arising from unexpected disruption of the critical systems and to have continuity in business activities. The disaster recovery plan includes off-site storage of valuable data and back up server(s) at an alternative location to continue business operations in the event of a major disaster. Keeping in view the criticality of UTS which provides continuous online processing of transactions on a real time basis and is a major source of revenue to IR, a duly tested, documented and comprehensive disaster recovery and business continuity plan and a ready-to-start reserve facility with offsite storage of important data is essential. Audit observed that:

- A disaster recovery and business continuity plan was not formulated and put in place in all the zones of IR. Failure to curb the high incidence of link failures as explained in paragraph 8.2 was partly due to the absence of a business continuity plan to address interruptions in service.
- Although back up servers were available, the mechanism of accessing the back up servers and the data stored in them were not tested leading to operational problems as detailed below:

- In SER it was noticed that tickets issued through Cal-2 (Back-up server) could not be cancelled through Cal-3 server. Even in ER, the two servers Cal-1 and Cal-2 were not integrated and therefore tickets issued through one server could not be accessed and cancelled using the other server.
- Similarly in NR, the system prevented field locations (New Delhi, Delhi, Nizamuddin, BVH) on 5 and 17 March 2007 and 3, 4, 6 and 7 April 2007 from canceling tickets from back up servers (DR servers). Further, when the main servers were down on 24 April 2007, booking from DR server could not be done and tickets were issued manually at Delhi, Ghaziabad and all other locations of the zonal server. This indicated that back up servers were not containing the entire data as a replicated copy of data residing on the primary server.
- UTS on CR and WCR failed (17 April 2006) from 0.05 hours and 8.50 hours due to server problem and the loss was assessed as Rs.50 lakh. Similarly, both the UTS primary and secondary server failed (5 February 2007 at 17.20 hrs) hampering the UTS operations in WR for over 50 minutes.
- In SCR, when the UTS/Secunderabad switched over to disaster recovery server (9 December 2006) located at Chennai from 10.00 to 11.00 hours all the locations in SCR were advised to log into MAS server of Chennai. But many locations were denied access to MAS server with messages like 'Invalid login name/pass word' 'remote end disconnected' etc. Only 25 locations were able to log into MAS server and issue UTS tickets. Even the locations that logged into MAS server could not generate cash summaries from UTS/MAS server for the transactions done between 10.00 to 11.00 hours. Further one location could not cancel the tickets issued from MAS server.
- Off site storage of data were also not provided in some zones (ECR and EcoR). In ECR, the back up data was stored in the same premises, exposing it to the same set of risks. In Dhanbad Division the booking data was lost due to computer viruses and UTS operations came to a halt for 15 days.

Thus, there was no disaster recovery and business continuity plans in the zones and the back up measures were not tested leading to operational problems of non-synchronisation of primary servers with the back up servers.

Recommendations

Railways should have a formal and documented disaster recovery and business continuity plan encompassing all factors relating to IT risks. The back up measures need to be tested on a regular basis to avoid problems of synchronisation of primary servers with the back up servers.

1.9.2 Inadequate IT security practices

Every organisation leveraging IT in a big way has an obligation to secure IT and related assets including data, applications and infrastructure to ensure confidentiality, integrity and availability of the information systems and communication systems that store, process and transmit data. It is imperative that physical and logical access and environmental controls are adequately provided for. The prevalent checks were inadequate as brought out below:

1.9.2.1 Inadequate physical access and environmental controls

Physical and environmental controls prevent unauthorised physical access and interference to IT services. UTS being a mission critical system, it is imperative that the computer equipment and the information contained therein are physically safeguarded with access only to authorised personnel and that the IT assets are properly maintained and adequately protected. Audit observed that:

- There was no effective mechanism to restrict entry of unauthorised persons to UTS locations where terminals, communication equipments, cash and other documents were kept and to the server rooms rendering the system vulnerable to disruption by unauthorised persons (SR, ECoR, WR, NR, NER, SECR and SER). Physical security of server room was also deficient (SR and WR).
- Neither security personnel were posted nor were any instruments installed to restrict unauthorised access in UTS locations over ECoR and SER. In NR, the biometric identification system installed at CCM/IT office buildings for controlling entry to the console room housing the zonal servers, was not in use.
- Costly equipment like routers, modems etc. deployed on UTS needed to be protected against water, dust etc. In CR, it was observed that at many locations, the booking offices were prone to water seepage. In one location, it was seen that the rain water dripped from the ceiling and affected the working at counters. Staff used containers to collect the water to prevent damage to printers, terminals etc. It was reported that the air conditioners provided to protect UTS equipment had to be replaced thrice due to water seepage at this location.

1.9.2.2 Inadequate logical access controls

The activity of management of access rights and assignment of privileges is done through 'User Definition Management' (UDM), a software utility. The creation of new user IDs, assigning privileges, modification of existing privileges and deletion of users are important activities under UDM. Requests for new user ID and changes required are proposed by supervisors of locations and the database administrator assigns the requisite privileges to the user.

Logical access to the UTS is to control and protect the applications and underlying data files from unauthorised access, amendment or deletion. The access is to be controlled by identifying each individual user through his/her

unique login ID which is also linked to the user rights and access to various areas of the application. The system provides for two very important operation level rights as given below:

Terminal Type	User Type	Rights
Booking	Booking	Enquiry/ Issue/Cancellation
Supervisor	Supervisor	Supervisory functions such as special cancellations in addition to all the above rights

It was observed that the controls which govern the management of user IDs and passwords were absent. This made the system vulnerable to unauthorised access and attendant problems relating to accountability as brought out below:

- Commercial clerks having booking privileges were allowed to login to the system with supervisory user ID/password to perform supervisory functions such as special cancellations (SR and SECR). Further, in some stations where chief booking supervisor was not available on all the shifts, it was observed that supervisory privileges were carried out by the booking clerks present on duty, which was an inherent risk. (CR, ECoR, SER and WCR). In five locations of ECoR, 18 staff members were allotted with both operator as well as supervisor privileges.
- In some locations, user IDs of commercial clerks, who went on long leave or were transferred to another booking location or retired from service were not deleted and the system was therefore prone to unauthorised access. (SR, SER and NER). In SR, some of the users IDs were used by the subsequent incumbents. User ID and password in many cases were the same resulting in one user logging into the system with user ID and password of another user. Passwords were shared amongst different users even in ER. In SR, duplicate users were created when user privileges were upgraded e.g. from operator to supervisor, supervisor to administrator etc. and hence, one user had two or more user IDs with different roles. In WR, it was found that 354 users of 57 locations had two or more IDs and in ER, one user had 12 IDs.
- As per functional specifications of the UTS, the length of all user passwords should be of 10 digit alphanumeric characters. Audit however observed that the maximum length of user passwords accepted by the system was only 6 digits. Moreover, there was no restriction on minimum length of password and system even accepted a single digit/character password (NR, NER, SER, SWR, ER, SECR and ECR). On being pointed out by Audit, the length of password was increased to four digits in Delhi UTS, which was till not as per functional specifications. In NR, multiple user IDs were created for some users as noticed at Moradabad and Ghaziabad locations. It was further observed that passwords were lying unencrypted in system tables in NR.
- On WCR, ER and ECoR, it was noticed that the user's passwords were not changed since installation of UTS at various locations.

Thus, the IT security practices were deficient with inadequate physical and logical access controls as a result of which the system was exposed to unauthorised access and the IT assets were not adequately protected.

Recommendations

IR should develop a comprehensive IT policy. Adequate physical access controls should be instituted to safeguard UTS assets and access controls should be strengthened to ensure accountability for transactions. Assignment of various privileges should be standardised and adequate controls need to be established to prevent misuse of privileges.

1.9.3 Deficient change management

A dynamic system such as UTS is based on the policies of the Government. From time to time, the framework of rules undergoes changes and these would need to be incorporated into the system in time. A sound change management procedure ensures that the requisite changes are made into the software in an authorised, accurate and timely fashion. Audit observed that:

- There was no documentation (for testing of changes, formal approval/authorisation before releasing new online versions) in many of the zones to trace the authenticity of changes made to UTS software from time to time. Further, it was seen in NR that even oral requests for changes in the application were accepted. As a consequence, changes to be made in the software were not analysed properly and often implemented incorrectly. For instance, while Railway Board had directed to reduce the fare of second class ordinary fare by one rupee (September 2005), a fare reduction of two rupees for combined tickets (Mail/express and ordinary tickets) was incorrectly incorporated in the program logic. Similarly while Railway Board reduced the second class fare by one rupee with effect from 1 April 2007 for non-superfast mail/express trains only, the changes were incorrectly made in the system to reduce the fare of superfast trains also apart from the fact that the changes were carried out after a delay of three months.
- The problems faced during the operation of UTS were referred to CRIS telephonically and the necessary modifications were carried out by CRIS without following proper documentation procedures (NEFR).
- The changes in tariffs were not carried out in the system in a timely manner resulting in improper levy of fares from passengers. While in some cases the changes were not effected at all, in others the changes were effected belatedly. For instance, in an important case of change of business rule affecting all the railway zones, second class fare of mail/express trains was reduced by one rupee with effect from 1 April 2007 necessitating superfast surcharge ticket to cost nine rupees for holders of mail/express tickets who traveled on superfast trains instead of eight rupees chargeable earlier. No changes have been made so far in the UTS versions operational in various other zones (ECR, SR, ECoR, ER, NER and SER) while the required change was made in the system after a delay of one month and 20 days in CR leading to short collection of fares from passengers. In SR

alone, the short collection of fares for two months i.e.; April and May 2007 was Rs.1.68 lakh. It was further seen in CR that five out of the 12 changes made in the system from January 2006 to May 2007 were done belatedly.

Similarly, even though the inflation in distance between Gooty-Dharmavaram section of Guntakal Division for charging fares were withdrawn (September 2006) the corresponding changes were not carried out in the system and the tickets issued from Bangalore Station to Bellary, Hospet, Gadag, Hubli etc. via Gooty-Dharmavaram Section continued to be issued with the inflated distance, resulting in levy of extra fares from passengers.

Thus, the mechanism to carry out changes in the software to be in line with the changes in the framework of rules was deficient as incorrect or delayed changes were carried out and were not documented.

Recommendations

IR should institute a mechanism for effecting changes to the program logic promptly and accurately as and when revisions in the business rules take place. IR should ensure that all changes are properly authenticated and documented.

1.9.4 Inadequate training

As training of booking clerks was a critical input for successful operation of UTS, all the zones were instructed (June 2003) to ensure proper training of staff on an urgent basis. Audit, however, observed that trained staff was not adequately available to man the UTS terminals in various zones. Training in various zones was to be imparted by CRIS. Audit observed inadequacies in providing training to staff in the zones as shown below.

- In WR, only 123 out of the strength of 534 were trained in UTS in the 20 locations test checked. Similarly in ECoR, only 14 staff members were trained as per records. During the course of audit at selected locations, the booking supervisors intimated that none of their staff members were trained.
- Only 34 staff members were trained for a day in three batches in SER despite three MoUs being signed with CRIS for Rs.11.90 lakh for imparting training to 230 persons in 23 batches in two phases apart from imparting training in 36 stations in the third phase. Most of the booking clerks in SWR were not trained and in NEFR, training in most cases was organised by deputing UTS operators from divisional headquarters for a very limited period, which was inadequate.
- Moreover, none of the audited locations were provided with user manuals leading to the risk of unauthorised practices being adopted by booking clerks (WR and SWR).

Thus, training of staff was not receiving the requisite importance and consequently the operational efficiency of the system was compromised.

Recommendations

IR should ensure that training is imparted to all the concerned staff in a time bound manner. Updated user manual should be made available at all UTS locations.

1.10 Application controls

Application controls ensure that the transactions are carried out according to the business rules of the organization. These controls contain validation checks to cover input, processing and output operations of the systems. Audit observed that a number of important validation controls for issue and cancellation of tickets, fares, definition of routes and issue of blank paper tickets were inadequate, data base had various deficiencies and the validation control for ticket rolls was inadequate as brought out below:

1.10.1 Inadequate validation control for tickets

Audit observed that validation for issue of advance journey tickets, cancellation of non-suburban unreserved tickets and for issue of season tickets was deficient as shown below:

1.10.1.1 Advance journey tickets

As per Joint Procedure Order between Commercial and Accounts departments, the system was designed to issue tickets three days in advance (excluding the day of journey) in case of non-suburban stations only which were located beyond 200 kilometers. Results of test data revealed that the system allowed issue of advance journey tickets for non-suburban stations as well for distances less than 200 Kilometers which was not permissible as per JPO (ECoR, SER and SECR).

1.10.1.2 Cancellation of unreserved tickets

As per rules¹ read with the Joint Procedure Order of Commercial and Accounting departments cancellation of non-suburban unreserved tickets is allowed up to three hours after departure of the last train, on designated day of journey, towards the destination for which ticket is issued. Audit observed that:

- The system improperly allowed cancellation of non-suburban tickets even after three hours of departure of last train for the booked destination on that day (ECoR and SER).
- This apart, the rule itself was prone to misuse and frauds in case of unreserved tickets issued for short destinations where a passenger could perform his journey in the morning and return to the ticket issuing station the same day and cancel the ticket (ECoR, SR, CR, SER, NER, ECR, SECR and NR). For instance, a ticket issued from Mumbai CST to Pune was valid up to three hours after the actual departure of the last train of the day for the destination station. While the distance between Mumbai to

¹ Rule 213.5 of IRCA Coaching Tariff No. 26 Part I (Vol. I)

Pune is 192 kilometers the travelling time is four hours approximately. There are a number of trains to commute between Mumbai and Pune everyday and the last train for Pune departs from Mumbai CST at 23.35 hours and as such the ticket could be cancelled up to 02.35 hours on next day. Hence the passenger could travel up to Pune and return back to Mumbai CST and could cancel the ticket for refund later in the day.

The possibility of misuse or fraud has further increased since Railway Board has permitted (February 2007) refund of tickets issued through UTS on the day of journey at the ticket issuing station or at any of its cluster stations. Zones have been vested (October 2003) with the responsibility of defining cluster stations for every city/town/metro.

- Further, instances were noticed in the database where the difference between journey date and cancellation date exceeded three days. Further, journey tickets issued for travel on the same day were shown as cancelled on days prior to the journey date in the computerised database (SR).

1.10.1.3 Season tickets

The system was designed to generate identity cards for persons seeking/holding season tickets. The unique identity card number generated by the system is recorded on the season ticket so that misuse of season tickets is prevented. Passengers travelling on season tickets are required to carry the identity card issued and produce it to ticket checking staff when demanded. Various deficiencies existed in the issue of season tickets. Audit observed that:

- The season tickets issued did not contain the identity card details of the holder in many cases. The columns earmarked for identity card number and name in the season ticket had irrelevant data. While the identity card number was shown as zero, the names were displayed as 'XYZ', 'WWW' etc. (SCR and NR) defeating the very purpose for which the identity cards were generated.
- Further, even though season tickets were not to be issued to children below five years of age, the system permitted issue of season tickets to children under the age of five years (SCR).
- As per extant rules, superfast surcharge should not be levied on season tickets issued for journeys on suburban trains. An analysis of data contained in the season ticket journal for the month of March 2007 in SCR indicated that superfast surcharge was collected even on season tickets issued for journeys on suburban trains.
- In 9575 cases of identity cards issued to seasonal ticket holders in NR, the destination and originating stations were the same and the dates of issue and validity were also found to be the same raising questions on data integrity.

Thus the validation controls for issue of advance journey tickets, cancellation of tickets and issue of season tickets were inadequate. The policy of allowing cancellation of non-suburban tickets up to three hours after the departure of

the last train on the designated date of travel was prone to misuse in case of travel to short destinations.

Recommendations

IR should rectify the system and strengthen the validation controls on issue of advance journey tickets, cancellation of tickets and season tickets. IR may review its policy on cancellation of tickets issued for short destination journeys to prevent misuse.

1.10.2 Inadequate validation of fares and distances

Audit observed that the validation of fares and distances was weak as shown below:

- Differences existed in the fare chargeable for milk vendor season tickets for various destinations from Talegaon vis-à-vis the fares computed by the system thereby forcing the booking clerks to issue blank paper tickets (CR). Cases were noticed in ER, where tickets (including platform tickets) were issued with abnormal fares and the concessions given on Privilege Ticket Orders (PTOs) were incorrect.
- There were differences in the distances recorded between stations in the route database as compared to the actual distances which led to undercharge / overcharge of fares. (SR, ER and WR). Differences in distance between pair of stations for the same route in UTS and in the PRS were seen in CR and ER. Similarly in ECoR, the distances entered in the system were incorrect. The distance indicated from Bhubaneswar to Howrah via CTC-KGP-TATA-BSP-NZM was 2527 kilometers instead of 2327 kilometers as correctly shown in PRS resulting in excess charge of Rs.10 per ticket generated by UTS. Similarly, distance from BBS to MFP via KGP-HWH is shown as 1039 kilometers instead of 1152 kilometers as shown in the PRS resulting in the fare collected being lower by Rs.14 per ticket.
- Discrepancies were noticed in the distances between the same pair of stations resulting in irregular computation of fare. In Danapur division of ECR, it was found that the fare from DHN to LKR was Rs.69 while the fare from LKR to DHN was Rs.73. In a simulation exercise done by audit, the system calculated a fare of Rs.101 from New Delhi to Panipat for sleeper class ticket whereas it was Rs.103 from Panipat to New Delhi though the distance recorded in the system was same in both directions (NR).

Thus, there were differences in the fares chargeable as per business rules and those charged by the system and distances adopted between stations were incorrect leading to incorrect levy of fares from passengers.

Recommendation

IR should immediately rectify the fares and distances adopted in the system so as to be in accordance with the business rules and to ensure correct levy of fares from passengers.

1.10.3 Inadequate validation of routes and blank paper tickets

Unreserved tickets could only be issued for stations which have pre-defined routes in the route database. Audit observed that

- Several routes were not defined in the database and therefore the journey tickets could not be issued for many stations through the system (SR, NEFR, ECR, NR, CR, ECoR and SER). In NEFR, some of the important routes involving stations viz. Ledo, Jorhat Town, Tihu etc. were not defined at New Tinsukia location. Similarly in NR, at least 60, 44 and 44 destination stations/routes originating from Lucknow, Bareilly and Raibareilly respectively were not defined in database and tickets to these destinations were prepared manually. Similar deficiencies were also noticed at Garhmukteshwar, Ambala city, Jalandhar city and Jalandhar Cantonment stations. In CR, it was observed that tickets from Lokmanya Tilak Terminus station to stations such as Raxual, Saharsa, Motihari, Singruli, Adra, Ulubaria, Farrukhabad and Fatehgarh could not be issued from the system. Further, train No. 6734 was introduced in November 2006. Since its route was not defined in the system, tickets for Manmad to Tirupati could not be done through the system despite heavy load of passengers on that route.
- Blank paper tickets were also issued for stations whose routes were not specified in the system. However, there was no provision in the software to validate the distance between two stations where route is not defined. Recording the distance was left to the manual discretion of operators, which could result in an incorrect levy of fares from passengers. In a simulation exercise done by audit in ECR, it was observed that while generating a second class blank paper ticket from Samastipur to Yeliyur -a station in Bangalore division, the system even accepted a distance of 10 kilometers and generated ticket valuing Rs.16. Similarly, the system accepted a distance of 50 kilometers with fare of Rs.24 while preparing a ticket in ordinary class from Danapur to Kottayam in Tiruvananthapuram division.
- Validation checks for issue of blank paper tickets were inadequate (ECoR and SER). Blank paper tickets could also be issued in respect of destination stations already defined in the system.

Thus, while several routes were not defined in the system preventing issue of tickets to destinations, the validation controls for issue of blank paper tickets were also inadequate.

Recommendation

IR should assess the completeness of master data on priority and incorporate all routes in the database. The control mechanism for issue of blank paper tickets may also be strengthened.

1.10.4 Inaccuracies in database

Master tables contain the basic data based on which the transactions in computerised system are processed. Information contained in the electronic databases contained several deficiencies as detailed below:

- A large number of duplicate station names in master stations table were found (ECoR, CR, NER and NR). For example, Ahmadpur Junction in ECR was having two station codes as ADP and AMP. Dehri-on-Sone was also appearing two times in the database having station code as DOS and DEI in Mughalsarai and Delhi divisions respectively. Conversely, it was observed in ER, that two stations (Kallayi in SR and Kulpi in ER) had the same station code 'KUL'.
- Incorrect station codes such as "AAAA" were found under Delhi division. Further, Delhi station had an incorrect station code as "BBBB" instead of "DLI". Various meaningless entries such as XXXXXX, AAAA, BBBB, etc were also found in the master station table (CR, ECR, NER, SR and NR).
- Additions of destination stations in master database were not being done as and when the stations were operational (CR, ECoR and SER).
- As per extant provisions in the codes, traffic earnings are to be apportioned amongst various zones on the basis of local and foreign traffic. Stations lying on other zonal railways (foreign traffic) were improperly marked as local stations which resulted in wrong apportionment of earnings among different zones. (ECR, CR, WCR, SWR, NR, and NWR).
- Date of journey was recorded as 'Null' in 52 records of the database while particulars like Station from, station to, transaction time etc. were recorded in database, indicating that the data stored was incomplete. (SR).
- Dummy concession codes allowing negative concessions of minus 50 per cent and minus 200 per cent were seen. Further, the minimum age for availing senior citizen concession was recorded as 12 years in the database (ECR and SECR).
- A comparison of daily statement of cancelled tickets on 21 November 2005 generated at New Delhi Railway station and zonal level statement of earnings of the same day indicated variations. While the number of tickets cancelled was indicated as 417 in the station level statement of New Delhi, the zonal statement indicated that the number of tickets cancelled at New Delhi station was 418. Similarly, station level statement indicated that net number of passengers booked were 44,548 whereas, as per zonal level statement, the figure was 44,544. Thus, output generated by the system was not reliable. Railway administration accepted the discrepancies (NR).

Thus, station names were duplicated with different station codes, stations were wrongly specified and the database contained various inconsistencies casting doubts on its reliability.

Recommendation

IR should rectify the inaccuracies in the database to enhance reliability of data and to render generation of meaningful reports.

1.10.5 Inadequate controls in maintaining ticket roll continuity

The system provides for generation of ticket roll continuity statement for verification of continuity of rolls on a daily or monthly basis and for ensuring proper accounting of tickets. A review of continuity statements generated by the system in various zones indicated the controls were inadequate as detailed below:

- There was no continuity in sequence of ticket numbers at various UTS locations (Guwahati, Katihar, New Tinsukia and Dimapur) in NEFR. The monthly continuity statement of Khurda Road Station of March 2007 in ECoR revealed that there was no continuity in ticket numbers in five ticket rolls. Even in SER, the number of tickets sold as depicted by the system did not tally with the number of tickets sold when calculated with reference to the ticket serial numbers indicating gaps in the ticket roll continuity. In SR also it was observed from continuity statement for 18 May 2007 of Calicut station that the commencing number of one row in the statement was the same as the closing number of previous row. Similarly, one ticket number was missing in the continuity statement for 11 April 2007 of Tirupathur Junction station.
- The continuity report of 20 November 2005 generated at New Delhi Railway Station (NR) revealed that ticket numbers from 007126001 to 007126090 were shown as used by two different operators. In CR also the continuity statements were not generated correctly on various occasions (Wadi, Karjat and Manmad stations). Similarly in ER, the continuity statements were erroneously generated in Santipur and Katwa stations where the ticket roll numbers appeared twice and their utilisation did not tally with the manual records maintained at these stations (Roll nos 17917 and 17943 of Santipur and 51626 of Katwa).
- Further, it was also seen that in many locations the ticket numbers were not pre-printed, tickets were incorrectly numbered, excess tickets were available in the ticket rolls and tickets were of poor quality and in torn condition (CR, SECR, NCR, SCR, NR, NER and WR).

Thus, the system was deficient in controls to monitor and check any fraudulent use of pre printed ticket stationery. There was no provision in the system to check the continuity of ticket rolls.

Recommendations

IR may strengthen its monitoring mechanism on use of the pre-printed ticket stationery. Validation checks may be built in the system to highlight cases of discontinuity in ticket rolls.

1.11 Conclusion

Indian Railways has implemented the Unreserved Ticketing System in phases in all the zones to harness the potential of Information Technology. The arrangements for acquisition through CRIS were predominantly characterised by delays and the communication channels provided by BSNL were frequently interrupted by extensive link failures. Indian Railways, however, did not have any structured mechanism in place to obtain minimum guaranteed services and consequently implementation of Unreserved Ticketing System over Indian Railways was delayed and provision of incessant services was hampered. The decision of the Indian Railways to acquire dot matrix printers for the locations covered in earlier phases, despite being aware of its vulnerabilities, rendered the system susceptible to misuse. The system was not comprehensively developed to encompass all the business rules requiring frequent manual interventions and thereby enhancing security risk apart from inconveniencing the passengers. The system was operated in an inadequately controlled environment as both physical and logical access controls were deficient, change management controls were weak and disaster recovery and business continuity plans were not formulated. Validation controls for issue of season tickets and cancellation of tickets were inadequate and the facility of cancellation of tickets for short destinations was prone to misuse. Fares and distances were incorrectly adopted leading to incorrect levy of fares from passengers. Master data was incomplete and contained inaccuracies. The control mechanism on use of ticket rolls was also deficient and there was ample scope for improvement.

Chapter 2 Other computerised applications in Indian Railways

2.1 IT Security on Western Railway

2.1.1 Highlights

Even 20 years after implementation of computerised applications in Western Railway, IT security policy was not laid down. Both the physical and logical access controls were inadequate exposing the systems to unauthorised access and malicious software. Western Railway Administration did not conduct any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk.

(Para Nos. 2.1.6.1 and 2.1.6.3)

Network security was inadequate as open ports were found in personal computers in Western Railway rendering the systems vulnerable to viruses and worms and intrusion by hackers. There was no mechanism to monitor and control internet usage of users.

(Para No.2.1.6.2)

Physical and information assets in Western Railway were not classified and there was no mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information. Training in IT security was inadequate and internal audit of IT assets, application and its security were not conducted.

(Para Nos.2.1.6.4, 2.1.6.6 and 2.1.6.7)

2.1.2 Recommendations

- Western Railway Administration should develop a proper IT security policy and assess the risks and vulnerabilities on priority basis.
- Western Railway Administration should continuously monitor the network traffic and system usage and institute adequate security controls- both physical and logical to safeguard IT assets, systems and data from external and internal threats.
- Internal audit of IT systems should be conducted. IS security training should be adequately imparted. Physical and information assets should be classified based on their sensitivity.

2.1.3 Introduction

IT Security encompasses understanding and management of risks involved, managing the network traffic and security, safeguarding IT assets, data, applications, infrastructure and personnel, selecting and implementing effective controls to ensure confidentiality, integrity and availability of the information and communication systems that store, process and transmit data. Dramatic increase in reported computer security incidents, ease of obtaining

and using hacking tools, steady advance in sophistication and effectiveness of attack technology and the dire warnings of new and more destructive cyber attacks etc., could affect the Railway's computer system.

2.1.4 Audit objective

The audit of IT security of the computerised applications in Western Railway was carried out with a view to assessing whether adequate and effective information security controls were implemented to protect confidentiality, integrity and availability of the systems and data.

2.1.5 Audit scope, criteria and methodology

IT Security audit was confined to assessing the security program management, which provides a framework for understanding the associated risks and instituting effective controls for mitigating the risks, network security management, access and change management controls.

Standard Information Security practices were used as audit criteria to evaluate the IT Security in Western Railway.

Relevant records, reports and documents relating to IT assets were analysed. Network security was analysed using network security scanner. A questionnaire was used to obtain information with regard to IS Security policy and other aspects apart from discussion with the users.

2.1.6 Audit findings

The IT Security audit of computerised applications in Western Railway disclosed inadequacies in IT Security, network security and traffic management, lack of risk assessment, non-classification of IT assets and information, inadequate change management and training, absence of internal audit of IT systems and inadequate management of business continuity process as brought out below:

2.1.6.1 Inadequate IT Security

A proper policy framework for IT security embodies adherence to strict norms and procedures in the system for ensuring confidentiality, integrity and availability of reliable and authentic information. Moreover, critical or sensitive business information processing facilities should be housed in secured areas, protected by defined perimeter security with appropriate security barriers and entry controls. Precautions are also required to prevent and detect malicious software since both the software and information processing facilities are vulnerable to introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. Audit observed that:

- Even after 20 years of implementation of computerised applications in Western Railway, IT security policy was not laid down by the Railway Administration. Absence of laid down security policy result in ineffective segregation of responsibility, absence of established performance centres and demarcated areas of operation.

- Physical security control weaknesses such as inadequate physical barriers and ineffective screening of visitors contributed to weakening the perimeter security at several facilities of the department exposing sensitive computer resources and data to unauthorised access.
- There was no mechanism to guard against internal threats (an action or event initiated by an employee or staff having valid access to information as part of performing his or her duties) to information security. In response to an audit questionnaire one (EDP centre) out of the seven departments stated that there was no loss caused by insider threats. A test check, however, disclosed that a temporary employee had misused the Passenger Reservation System (PRS) facility by issuing reserved tickets to passengers against seats already allotted to other passengers, which was discovered in the train when there were ten passengers for five seats.
- Inadequate logical access controls reduced the reliability of department's computerised data and increased the risk of unauthorised disclosure and modification. It was seen that IP addresses were misused by staff to access the internet network. A test check further disclosed that five out of twelve PC's connected to Railnet could be opened using the administrator's account without a password.
- Personal computers installed in various departments did not have the latest antivirus definition files nor were the staff aware of antivirus definition files to be downloaded through the internet. Railway Administration accepted that personal computers connected to Railnet were affected by virus.
- There was no filtering mechanism to restrict users from downloading malicious content on computers. This coupled with poor physical controls exposed the system to malicious software and rendered the system vulnerable to frequent break downs.

2.1.6.2 Inadequate network management

Network management includes management of network security and traffic. Network security management encompasses deployment, maintenance and monitoring of the effectiveness of network security controls to safeguard information and information systems and protect supporting network infrastructure. Effective network security management practices also require established and documented procedures that provide instructions for the system to restart and recover in the event of system failure in a short time. Further, to manage network traffic effectively network devices have to be configured correctly. Audit observed inadequacies in the network security and traffic management as brought out below:

- In a test check conducted on 12 January 2007 using GFI LANGUARD Network security scanner and on 08 June 2007 using Network Security Auditor (NS Auditor), it was noticed that ten ports were open in the personal computers connected to Railnet, exposing the users of the system to risks as mentioned below apart from penetration of viruses and worms in servers and personal computers and other intrusion by hackers.

Type of risk	Impact
Denial of Service on Port 135	The usage of Central Processing Unit (CPU) could be raised up to 100% by telnetting to port 135 and irrelevant data/characters could be input.
OOB denial of Service	An attacker can send a custom packet causing the system to stop responding.
Teardrop denial of service	An attacker can send a custom UDP packet causing the system to stop responding.
Land denial of service	An attacker can send a custom packet causing the system to stop responding. The source code written in 'C' language is also available on the internet.

- Railway administration did not have a mechanism (either by installation of hardware or software) to monitor and control internet usage of users. On scrutiny of files, Audit noticed that some users of Railnet in Western Railway had downloaded and uploaded voluminous data (of 5.3 GB and 3.3 GB respectively) resulting in wastage of time besides denial of Internet service to other genuine users.

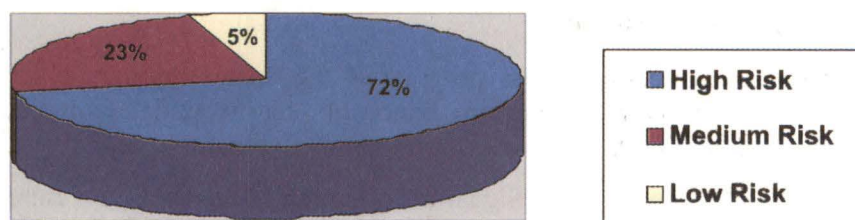
Railway Administration stated that there was no system to monitor the pattern of usage by individual users and as a result cyber slacking¹ could go uncontrolled.

2.1.6.3 Lack of risk assessment

Risk assessment is essential for risk management and overall security programme. This assists in identification of security risks and institution of effective controls. Audit observed that:

- Railway Administration has not performed any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit in 3com switch (Host IP 10.3.3.103) using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk (for e.g. Cross-site scripting, Avenger's News system command Execution, Directory transversal vulnerability, Remote command execution, Web_store and cgi etc) 63 were of medium risk and 14 were of low risk. Railway Administration accepted that automated tools were not identified to scan and monitor the network and host devices.

¹ practice of employees using the Internet or other employer-provided resources for leisure during work hours, contributing to inefficiency



2.1.6.4 Absence of classification of IT assets and information

Physical and information assets should be classified to indicate the need, priorities and to provide proper degree of protection. Information and physical assets have varying degrees of sensitivity and criticality. As per the IT Security standards, the information may be classified as unclassified, operational use only, private, restricted and confidential. Audit observed that:

- There is no centralised inventory of critical information and systems maintained by the Railway administration. Test check of the Stores & Signal & Telecommunication department revealed that inventory database was also not maintained department wise. In these circumstances, the Railway administration may not be in a position to do proper asset classification of the system based on the importance and sensitivity of the system/data in use, indicating lack of effective control.
- In spite of incurring expenditure of the order of Rs.32.06 crore during the last three years on acquisition of IT assets, the assets were neither classified nor was there a mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information.

2.1.6.5 Inadequate change management

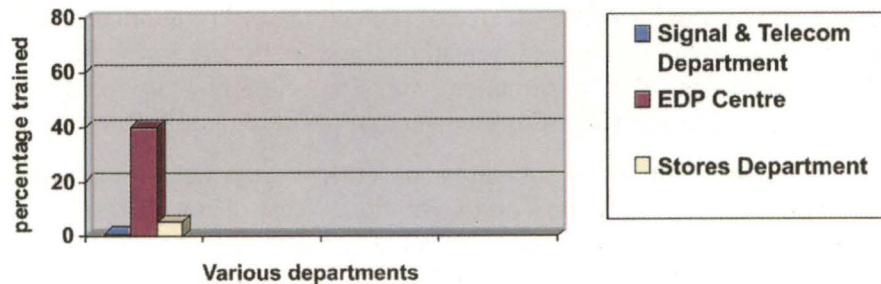
Established change management practices/ procedures are required to ensure that unauthorised changes are not carried out to the system. This should ensure only approved changes are incorporated in the programme and in time. Audit observed that:

- Changes in the system necessitated due to change in introduction of rules were not carried out in a timely fashion resulting in inconvenience to the traveling public as well as increasing the risk of loss of revenue to the Railways. For instance pursuant to Government of India notification of March 2006 regarding introduction of service tax on catering services on board the trains of Indian Railways, service tax for catering service on Rajdhani/ Shatabdi trains was not updated immediately in the fare structure resulting in short recovery of Rs.0.42 crore for the period from 1 April 2006 to 31 May 2006. Railway Administration stated that this has since (June 2006) been introduced after obtaining necessary instructions from Railway Board.
- No records were maintained to indicate the requests for change and the changes carried out in the system.

2.1.6.6 Inadequate training

An effective security awareness program is the means through which the organisation communicates the importance of security policies, procedures and responsibilities to its employees. Audit observed that:

- Out of three departments (Signal & Telecommunication, EDP centre and Stores), training in IT security awareness was imparted only in the EDP centre. Even in the EDP Centre, only 10 out of 25 employees were trained in security awareness. In the other two departments only basic training (use of Login & password) was imparted, which was inadequate.



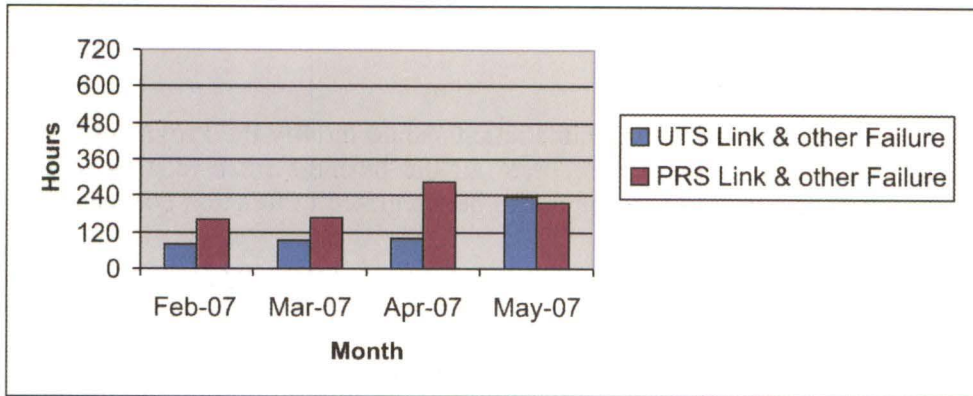
2.1.6.7 Absence of internal audit of IT systems

Internal audit assists in providing an assurance that safeguards are adequate and in alerting the administration to potential problems and threats. Audit noticed that Railway Administration has not covered internal audit of IT assets, application and its security in the annual inspection programme and hence internal audit of IT assets, application and its security has not been done so far.

2.1.6.8 Inadequate management of business continuity process

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. The business continuity plan should be tested regularly to ensure that they are updated and periodically reviewed for their continuing effectiveness. Audit observed that:

- There was no managed process for developing and maintaining business continuity throughout the organization, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.
- Link failures in UTS and PRS were not addressed on time resulting in disruption of service. A test check in audit of link failure for a period of four months at major locations revealed that link failures ranged from 10 minutes to 54 hours (minimum at Vapi station and maximum at Vasai station) in UTS and from 10 minutes to 20 hours and 30 minutes (minimum at Malad station and maximum at Okha station) in PRS respectively. The link showed an increasing trend, reflecting that there was no appropriate contingency plan to minimise the impact of this failure.



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:

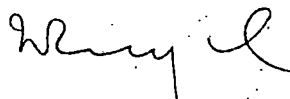
- The control procedures were not manualised.
- Training was not provided to employees regarding operation of system and security awareness.
- User ids and passwords were shared by the users irrespective of their duties.
- No audit trail was maintained.
- To maintain data integrity, edition/deletion 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)

Deputy Comptroller and Auditor General

New Delhi

Dated: 11th April, 2008

Countersigned



(VINOD RAI)

Comptroller and Auditor General of India

New Delhi

Dated: 11th April, 2008

