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)**.