3.2 Implementation of information technology in the Integrated Bus Reservation System in Maharashtra State Road Transport Corporation

Highlights

The Corporation did not invite open tenders for procurement of hardware.

(Paragraph 3.2.5)

There was under realisation of revenue of Rs.16.50 crore due to incorporation of unauthorised computation rules.

(Paragraph 3.2.6)

Database was not designed to capture critical data and appropriate validation checks were not incorporated.

(Paragraphs 3.2.7-3.2.8)

A concession of Rs.52.88 lakh was granted under an unauthorised miscellaneous concession code.

(Paragraph 3.2.9)

Due to non-incorporation of audit trails, unauthorised access, modification of data and programs cannot be detected.

(Paragraph 3.2.11)

Assignment of common identity for all users instead of having a unique identity for each user rendered the system vulnerable to misuse.

(Paragraph 3.2.14)

Frequent breakdowns of leased lines resulted in unwarranted expenditure of Rs.15.05 lakh.

(Paragraph 3.2.16)

Due to absence of business continuity plan and standby system, the integrated bus reservation system is vulnerable to serious disruption.

(Paragraph 3.2.17)

Introduction

3.2.1 Maharashtra State Road Transport Corporation (Corporation) was established in 1961 under the State Road Transport Corporations (SRTC) Act, 1950. To facilitate passenger reservation, the Corporation has an online passenger reservation system known as Integrated Bus Reservation System (IBRS).

Organisational set up

3.2.2 The information technology (IT) needs of the Corporation are overseen by the electronic data processing (EDP) Centre at Head Office, Mumbai. EDP is headed by a Deputy General Manager (EDP) who is assisted by Senior Programmers, Junior Programmers and Data Processing Officers. The EDP Centre is responsible for the implementation and maintenance of the IBRS which functions under the Financial Adviser and Chief Accounts Officer.

Scope and methodology of Audit

3.2.3 During October 2003 to April 2004, audit reviewed general IT controls that control the design, security and use of computer programs in the Corporation and IT application controls specific to computerised IBRS and evaluated the effectiveness of the system in achieving organisational objectives. Taking into account various policy guidelines, circulars, tariff rules, fare revision, concessions offered *etc.,* business logic queries were developed which were converted into Structured Query Language (SQL) and run on data of the IBRS pertaining to the period November 2001 to December 2003 with the assistance of authorised EDP staff of the Corporation.

Integrated Bus Reservation System

3.2.4 The online reservation system (IBRS) was first implemented through a proprietary[1] mainframe system in 1988 using Cobol[9] platform, which was reengineered during 1996-97 using Oracle RDBMS platform as back end and Forms Library as front end. The IBRS facility is available for all the buses originating from Mumbai (including Thane) and Pune. The database is maintained in a server at one location each in Mumbai and Pune respectively. While terminals installed at Mumbai centre are connected to the server using local terminal server (LTS), the terminals installed at six reservation centres[2]

[1] ICIM 6080
[9] Cobol – Common business oriented language.
 RDBMS - Relational data base management system.
[2] Parel, Kurla, Dadar, Borivali, Vashi and Thane.

are connected to the Mumbai server through dedicated leased data circuit lines. In addition, reservation facilities have been provided through dial up telephone lines to four private booking agents[3] situated in suburban areas at Mumbai. Similar arrangements exist at Pune with five reservation centres[4] and six private booking agents[5] in suburban areas. The Pune and Mumbai servers are connected to each other through dedicated leased lines.

Audit observations on IBRS

System acquisition, development and implementation

3.2.5 The Corporation, violating the transparency requirements of open tenders, invited limited tenders only from two vendors M/s. International Computers Indian Manufacture Limited (ICIM) and M/s. CMS Computer Private Limited. A purchase order (April 1996) for supply of hardware[6] was placed with ICIM, Mumbai for Rs.35.02 lakh even though their past performance was not satisfactory as there were slippages in development of software in an earlier order. A purchase order for development of application software in RDBMS platform and work group server was placed at a cost of Rs.14.57 lakh with M/s. Neo Computers, a subcontractor of ICIM. Though there was a delay of 13 months in the delivery of software, the Corporation did not impose any penalty.

The Corporation stated that Rs.2.52 lakh was withheld by not paying annual maintenance charges. The reply is not tenable as no penalty was charged as per terms of contract.

Phase wise testing was not done; certification from competent authority was not obtained.

Audit also observed that systematic phase wise testing and stage wise check off were not done to enable proper evaluation of each stage of system development and no documentation was maintained.

The Corporation stated (August 2004) that proper care would be taken in future.

Unauthorised computation rules

3.2.6 The fare to be collected from a passenger is dependent on the number of stages travelled. Given a starting point and a destination, the number of stages are decided on the basis of one stage for every six kms to be stretched up to next 0.7 km for in between stops and maximum of next 1.3 kms for ultimate destination.

Audit noticed that this was not implemented in practice and the number of stages for which a passenger is charged is generally lower than the number of stages actually travelled. Using SQL, Audit noticed that in respect of long

[3] Vile Parle, Goregaon, Kandivali and Malad.
[4] Swargate, Shivajinagar, Pune Station, Pimpri Chinchwad, and Deccan.
[5] Aundh, Singhgad Road, Kothrud, Nigdi, Paud Road and Bhusari Colony.
[6] Team server with SCO Unix operating system.

There was under realisation of revenue of Rs.16.50 crore due to incorporation of unauthorised computation rules.

distance (LD) and middle long distance (MLD) services departing from Mumbai Central and Pune, there was shortfall in fixing of chargeable stages in respect of 12,157 bus stops for the period January 2001 to December 2003. This resulted in under charging of fares and consequent loss of revenue of Rs.16.50 crore[7].

The Corporation while confirming the above facts stated (August 2004) that stretching of stages may be necessitated by many factors such as (a) bifurcating of route from state/national highway to interior routes, (b) coinciding of stages point of various routes, (c) considering important alighting/boarding stops, villages, towns *etc*. The reply was not tenable, as the Corporation did not furnish any authority such as Government/Board of Directors' resolution, circulars permitting the stretching of stages beyond prescribed limits stated above.

The Corporation also stated that detailed examination of these issues will be taken up and necessary action will be taken accordingly.

Defective table design

3.2.7 The Corporation offers 100 *per cent* concessional fare to freedom fighters, Dalit Mitras,[] authorised press reporters, employees *etc*. Audit observed that the number of passengers who availed the above concessions between January 2001 and December 2003 was 1,33,526 and the monetary value of the concessions so availed was Rs.2.18 crore. Audit also observed that the database was not designed to capture data such as identity number, pass number, date of issue, validity period of pass, authorisation details, family details of employees, depot where passes were issued *etc*. In the absence of above data, the system was prone to misuse.

Database was not designed to capture critical data.

Audit also observed that the 'name' field accepted numeric characters. It was evident that user requirements were not properly assessed while designing the table structure. In view of the large number of passengers and the money value involved, capture of important data is critical for information as well as for analysis of the concessional scheme.

The Corporation, while confirming the above facts and figures stated (September 2004) that necessary action would be taken to capture such critical data in the new system.

Lack of preventive validation checks/controls

3.2.8 Audit observed that important validation checks/controls, which are necessary to prevent misuse of the system, were not incorporated in the application as is evident from the following examples:

---

[7] Based on a conservative 50 *per cent* load factor for the number of days the bus services were operated during the period November 2001 to March 2004.

[] The persons who have received Dalit Mitra (friend of backward person) award from State Government.

Appropriate validation checks were not incorporated.

- Passengers whose age was less than 60 years (*i.e.* date of birth after 1943) and minors (*i.e.* age <15 years) were granted 100 *per cent* concession in fare as freedom fighters.

- As per business rules, a Dalit Mitra is eligible for only one escort. Audit, however, observed that often more than two persons were allowed to travel on the same ticket.

It is evident that preventive validation checks were neither incorporated in the IBRS system nor exercised by the booking clerks at the booking centres.

The Corporation stated that necessary validation checks would be provided in the software and instructions would also be issued to the booking clerks.

Unauthorised 'MS' code used for grant of concession

3.2.9 Audit noticed that a miscellaneous concession code (MS) was created in the concession table wherein 100 *per cent* concession was granted and 34,543 passengers availed 100 *per cent* concession aggregating Rs.52.88 lakh under this category for the period November 2001 to December 2003. However, there was no authorisation for creation of this code for grant of 100 *per cent* concession and consequently no eligibility criteria was fixed for grant of such concessions by the Corporation. The grant of above concession was left entirely to the discretion of the data entry clerk at the reservation counter without any validation checks. Thus, it is clear that the IBRS database was vulnerable to manipulation, which, in the absence of any logs and trails cannot be traced.

A concession of Rs.52.88 lakh was granted under an unauthorised code.

Feedback from user department was not obtained for changes carried out.

The Corporation stated that the matter of deletion of the said concession code would be taken up with the traffic department. Moreover, critical information system such as IBRS requires a sound change management procedure for recording and performing changes. It was also observed that EDP officials interpreted the various circulars and incorporated the required changes in the IBRS system without formally involving the user department responsible for the implementation of Board's directives. Although sample cases of major changes were sent to the user department there was no system of formal certification from the user department for proper feedback.

The Corporation stated that such formal certification from user department would be obtained in future.

Lack of supplementary checks

3.2.10 Audit noticed that, apart from the deficiencies in the application software as stated above, even manual supplementary checks were lacking as seen from the following examples:

- Employees were permitted to book tickets without pass or beyond expiry date of pass. The Corporation stated that necessary validation checks would be incorporated.

- During travel, conductors are required to verify the identity and authenticity of the concession holders by verifying the identity card, pass/coupon number issued by the respective depots and enter such details in the way bills for further check at the depot level. Audit, however, observed that the above details were not entered in 1,095 waybills verified**.** The Corporation stated (September 2004) that instructions for recording the details of concessions on the waybill have been issued vide department circular No.25/2004 dated 2 September 2004.

- Family members of employees are eligible for free travel passes. As the employee is not mandatorily required to travel with the family and the pass is valid for travel anywhere in Maharashtra for one month, the present practice of not issuing family identity cards is not foolproof. No photo identity cards are issued. In the absence of such photo identity cards for families, it is not clear as to how the Corporation ensures that only bonafide family members avail of this concession. Audit further observed that conductors did not enter travel details in the pass. In the absence of such details, the Corporation will not be able to restrict travel to the prescribed limit. The Corporation stated (August 2004) that it would examine the possibility of issuing photo identity cards. It also stated that necessary instructions would be issued to the conductors for recording the details of travel in the pass.

Family photo identity cards were not issued and hence passes were vulnerable to misuse.

Audit trails not incorporated

3.2.11 As per the system requirement specifications (SRS) and terms of contract, the vendor was to incorporate Master Audit Trail Reports and Other Transaction Reports in the application software. Audit observed that audit/system logs were not incorporated in the software. In the absence of audit trails and system logs, unauthorised access, modification to data, programs, table structure cannot be detected and the person responsible for such unauthorised access and modification cannot be identified.

Unauthorised access, modification of data/ programmes cannot be detected due to non-incorporation of audit trails.

The Corporation stated (August 2004) that audit trails were not incorporated, as it would affect the response time resulting in delay in issue of tickets to the passengers as well as limited hard disk capacity. The reply is not satisfactory as audit trails are an important and integral part of any IT application and the system response time criterion should have been met without compromising on the audit trail. Creation and maintenance of audit trails is relevant in the view of unauthorised creation of code wherein 100 *per cent* concession of Rs.52.88 lakh was granted, as detailed in paragraph 3.2.9.

The Corporation stated (August 2004) that such audit trails will be incorporated in the new software under development.

Private booking agents

3.2.12 To safeguard the Corporation's financial interests, booking by private agents is to be restricted to the extent of security deposit held by the Corporation. Audit noticed that proper validation checks were not incorporated to limit ticket booking by private agents to the extent of security

There was lack of system controls on booking by private agents.

deposit held by the Corporation. Consequently, it could not prevent overbooking by four private agents who subsequently defaulted in paying Rs.6.46 lakh. The Corporation accepted (August 2004) that at present there is no provision in the IBRS to check the amount receivable from private booking agents and stated that necessary checks would be incorporated in consultation with user departments. It also stated that it had recovered Rs.5.65 lakh (principal Rs.4.98, interest Rs.0.67 lakh) and balance principal of Rs.1.48 lakh was yet to be recovered.

Non generation of report on balance fare to be collected

3.2.13 The IBRS system did not provide for generation of critical information on the balance fare to be collected whenever fare is revised from the passengers who had availed advance reservation facility prior to revision of fares. A query to generate the above information revealed that 1,47,754 passengers availed advance reservation through the IBRS system and money value of differential fares to be collected was Rs.11.04 lakh as per IBRS system. In the absence of such reports, there is no mechanism to verify whether conductors have collected the balance fare.

The Corporation stated (August 2004) that necessary care would be taken to generate such reports in the future.

System security

3.2.14 Lack of segregation of duties, password, operating and application security controls

IBRS was vulnerable to unauthorised access/modification.

- General users such as punch operators, programmers, computer operators were also granted roles as Data Base Administrator/Divisional Traffic Officer (DBA/DTO). This arrangement is not in conformity with the need for segregation of duties. The user ID was the same for all the booking centres.

The Corporation stated (August 2004) that such logins were maintained for effective operation of the system. The reply is not acceptable as this practice adversely affected the security in a revenue generating application.

- Unix login for access to the IBRS source code was too generic and all persons having access to the source code shared the same password. Persons who had resigned/transferred to another department continued to have user access as DBA/DTO. Even the software vendor who developed the software in 1997 continued to have user access. The Corporation stated (August 2004) that necessary action would be taken.

- Even single character was accepted as password. Normal password control procedures of automatic lapse of password after a predefined period to facilitate periodic change of passwords were non-existent. In the absence of system logs, security breaches cannot be detected. The

Corporation while confirming the above facts stated (August 2004) that it would do the needful.

- Audit observed that the IBRS system lacked physical security as the main server was placed at the entrance of a common room in the EDP centre where visitors and staff of other departments had easy access. The Corporation stated (August 2004) that necessary care would be taken to place the server in a separate room.

Deficiencies in networking security

3.2.15 Audit observed that:

No firewalls, intrusion detection system were installed.

- No firewalls, intrusion detection system, network management software to support fault management, traffic management/monitoring, access control management and security management *etc*. were installed in the IBRS. The Corporation stated (August 2004) that the same would be provided in future.

IBRS was vulnerable to unauthorised access through dial up modem due to inadequate security features.

- The current dial up facility requires dialling in the telephone number and password only. There was no procedure for dial back *i.e.* terminal/ token-based authentication system provided to private booking agents. The system is thus vulnerable to unauthorised access as any person even with little IT skills and utilities can access the database of IBRS system from anywhere through dial up modem. This vulnerability was further compounded as the data is transmitted in the network in unencrypted form. The Corporation while confirming the above facts stated (August 2004) that necessary care would be taken in the new system.

Breakdown of networking equipments

3.2.16 Breakdown of networking equipments results in denial of services. Audit observed that the service level agreement for networking did not specify any benchmark for the frequency of breakdowns and the maximum time within which the system was to be restored failing which penalty was to be levied. Due to frequent breakdowns of leased lines, connectivity had to be established through dial up facility resulting in unwarranted expenditure of Rs.15.05 lakh.

Frequent breakdowns of leased lines resulted in unwarranted expenditure of Rs.15.05 lakh.

The Corporation while confirming the above facts stated (August 2004) that no service level agreement was entered into with the service provider, MTNL/BSNL being Government agencies. The reply is not tenable as service level agreement should have been entered into to ensure better service.

Absence of business continuity plan

3.2.17 The Corporation had not documented 'disaster recovery and business continuity plan' outlining the action to be undertaken immediately after a disaster and to effectively ensure that information processing capability can

be resumed at the earliest. Emergency hot sites, correct/current version of system software *etc.,* important for recovery from disaster, were not identified and documented. Audit noticed that there is no standby system. Consequently, when there was a data crash in October 2001, back up data since inception up to October 2001 could not be recovered. Subsequently, *i.e.* even after the crash, Audit observed that although backups of IBRS data were being taken at periodic intervals, there was no practice of offsite storage of backups. Further, there was no formal policy regarding the frequency of testing the backups or maintaining logs to verify any such tests. Though there was an annual maintenance contract worth Rs.3.00 lakh for the period June 1999 to January 2002 with the software developer (M/s. Neo Computers), there was no formal commitment for Oracle support. In the absence of formal commitment, M/s. Neo Computers could not be legally bound.

The matter was reported to the Government (May 2004); their reply had not been received (December 2004).

Conclusion

The Integrated Bus Reservation System, an online wide area networking system, had poor networking, operating, application and database security features and was hence vulnerable to unauthorised access and data/source code modification. These deficiencies had security implications in the absence of audit trails, system logs. Unauthorised business rule having bearing on the revenues of the Corporation was incorporated in the software. The database was not designed to capture critical data for grant of various concessions and validation checks were inadequate.

There is an urgent need to improve networking, operating, application and data base security features of the system.