CHAPTER III
INFORMATION TECHNOLOGY AUDIT

Information Technology Audit of Chennai Telephones Billing System

HIGHLIGHTS

∗ **Chennai Telephone Billing System (CTBS) is a non-integrated billing system used by the Chennai Telephones District (CTD), which could not make full use of Information Technology in ensuring timely and accurate billing by minimizing unaddressed bills and expediting the processing of advice notes and disconnections.**

(Paragraph 3.6.1)

∗ **During the period April 2002 to March 2005, 26,198 unaddressed bills amounting to Rs 3.83 crore were generated, which remained unpaid till August 2005. There were 9,190 unaddressed bills valuing Rs 1.57 crore which were pending for more than three billing cycles.**

(Paragraph 3.6.3)

∗ **During the period April 2002 to July 2005, potential revenue worth Rs 5.49 crore could not be generated due to delays in processing advice notes.**

(Paragraph 3.6.4)

∗ **Delays in disconnections resulted in accumulation of dues of Rs 8.03 crore.**

(Paragraph 3.6.5)

∗ **Inadequate Contract Management resulted in delays in implementation of the project. Moreover, certain important segments such as billing of leased circuits and I-Net could not be implemented due to deficiencies in firming up of the System Requirement Specification.**

(Paragraph 3.6.6)

∗ **Data migration from the old COBOL package to CTBS was not complete inasmuch as deposit data of the pre-CTBS period were kept in suspense status entailing manual intervention for refunds.**

(Paragraph 3.7.1)

∗ **CTBS failed to bill telephone connections, which registered 14.65 lakh metered calls from January 2003 to March 2005. Also, 2.37 lakh local calls and trunk calls amounting to Rs 2.92 lakh registered in ISDN child numbers were not billed.**

(Paragraph 3.8.1)

∗ **CTBS did not bill phonograms worth Rs 14.37 lakh despite the availability of the required inputs.**

(Paragraph 3.8.2)

∗ **Processing of rental rebates for faulty lines and billing of service tax from non-exempted subscribers could not be done in certain cases because of weak internal controls.**

(Paragraph 3.8.3)

∗ **IT security related control measures were not adequate.**

(Paragraph 3.9.2, 3.9.3 and 3.9.4)

∗ **CTD did not have a proper disaster recovery and contingency plan for business continuity.**

(Paragraph 3.9.6)

LIST OF RECOMMENDATIONS

✍ **The Company should strive towards having a standard integrated billing software for all its circles. For this purpose, the process of switching over to Call Detail Records (CDR) based billing system initiated in 2002, should be expedited. Pending introduction of the CDR based billing system, CTD should attempt on-line integration of CTBS with the existing commercial application software like CANMAPS, FRS[*], etc, after a proper cost-benefit analysis.**

✍ **The facility available in CTBS for linking of unaddressed bills and consumer numbers should be enabled immediately for minimizing unaddressed bills.**

✍ **CTD should enable online access of disconnection lists to ensure timely disconnections.**

✍ **CTD should incorporate billing of leased circuits and I-Net in CTBS**

---

[*] Fault Repair System

 ✏ **The Company should issue instructions, clearly specifying the IT system development methodology to be adopted by its units. These instructions should invariably include detailed steps to be followed for stages like project initiation, user requirement specifications, system requirement specifications, system design and acceptance testing.**

 ✏ **The Company should ensure that implementation plans of IT projects are well defined and the results of implementation are well documented to facilitate change management and business process reengineering at later dates.**

 ✏ **CTD should urgently validate the deposit details available in CTBS.**

 ✏ **CTD should examine the reasons for non-billing of telephone connections in spite of availability of the required inputs, and rectify the deficiencies. The reconciliation procedures should be strengthened.**

 ✏ **CTBS should be re-engineered for more effective validation checks to ensure data integrity and introduction of exception reporting mechanism.**

 ✏ **An internal audit team should regularly audit the database.**

 ✏ **CTD should formulate and implement an IT security policy and review it periodically.**

 ✏ **Logical access controls of CTBS should be strengthened by adequate logging of changes to critical data like master data, meter readings, etc. The audit trail function should be activated.**

 ✏ **CTD should ensure proper segregation of duties between the Data Base Administrator and the System Administrator.**

 ✏ **CTD should maintain an offsite storage location for backup data.**

 ✏ **CTD should formulate policies for anti virus, data backup and prepare a 'Business Continuity Plan' and 'Disaster Recovery Plan', for early implementation.**

 ✏ **CTD should prepare a plan for alternate arrangements for personnel in contingent situations.**

3.1   INTRODUCTION

Chennai Telephone District (CTD) under Bharat Sanchar Nigam Limited (Company) is one of the biggest telephone districts with 10.02 lakh working lines as of March 2005. The revenue from Landlines and Wireless in Local Loop (WLL) lines is billed and accounted for through a computerized billing system, viz., the Chennai Telephone Billing System (CTBS), commissioned in February 2002. The system generates up to 6.85 lakh bills every month. The

amount billed during 2004-2005 was to the tune of Rs 1153 crore. CTBS functions in a client/server environment on Oracle Relational Database Management System (RDBMS) with a Sun Solaris operating system.

A diagrammatic representation of the billing system of CTD is given below:
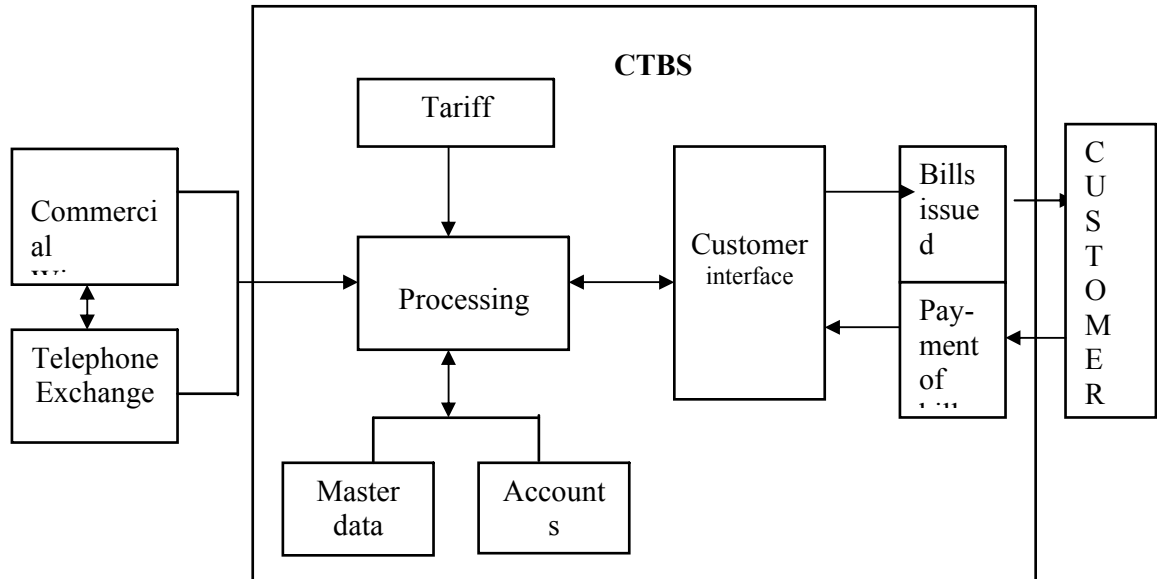
The Commercial wing authorizes the provision of telephone connections through Advice Notes (ANs), that are issued to the telephone exchanges for execution. Processing and monitoring of ANs in the Commercial wing is carried out by another software viz. the Commercial Advice Note Monitoring and Processing System (CANMAPS). Completed ANs, containing details of consumer number, address, telephone number etc., which form the basis for creating master data for billing the consumers, are transferred from CANMAPS to CTBS on a fortnightly basis through a file transfer protocol. Details of meter readings, trunk calls, etc are received from the exchanges. With this data and tariff details stored in the database, CTBS generates bills for rent, call charges and other dues.

The General Manager (GM), Telephone Revenue (TR), CTD is in charge of billing and accounting under the overall charge of the Chief General Manager (CGM), CTD. The GM (TR) is assisted by the Deputy General Manager (TR), Chief Accounts Officer (TR) and Chief Accounts Officer (Computer). The Organizational chart of the TR wing of CTD is given at Appendix-XV.

3.2   SCOPE OF AUDIT

The COBOL based billing package of CTD was replaced by CTBS in February 2002. Audit reviewed the development and implementation of the new system and its functioning for the period February 2002 to March 2005.

3.3 AUDIT OBJECTIVES

Whether the :
* System development methodology was in line with the requirements of computerization;
* Selection of technology was appropriate;
* System was implemented properly; and
* System was functioning in an economical, efficient and effective manner.

3.4 AUDIT CRITERIA

The main criteria used for audit were as follows:
* Standard business practices for Information Technology (IT) System development and implementation.
* Adequate validation checks to ensure completeness and accuracy of bills issued and accounting thereof.
* Adequate internal control mechanism to detect and plug revenue leakages.
* Standard IT security controls.
* Availability of trained personnel to ensure smooth and efficient functioning of the billing system.

3.5 AUDIT METHODOLOGY

During the Information Technology Audit of CTBS the CoBIT* framework was utilised. Audit adopted system based techniques like use of CTBS menu facilities, SQL[1] for queries and data analysis through spreadsheets for evaluating the performance of the billing system against the audit criteria broadly outlined earlier.

3.6 AUDIT FINDINGS

Ideally, a telephone billing system should ensure complete, accurate and timely billing and accounting. To accomplish this objective, the system should ensure that the basic data needed for billing are created and maintained properly in a secure manner. The system should check and validate the inputs and monitor the outputs to ensure correct and prompt billing. The controls around the system i.e the monitoring mechanism should be strong.

In order to achieve the above, it is imperative that the System Development methodology adopted is sound, the implementation is effective and the functioning is efficient. Audit observed that although CTBS served the needs of billing, certain deficiencies needed to be addressed for improvement in its functioning. Also, the Management needs to take into account the experience gained from the implementation of CTBS, while planning and implementing the future billing projects.

---

* Control Objectives for Information and related Technology – Audit framework followed by Information Systems Audit and Control Association (ISACA)
[1] Structured Query Language

3.6.1 INADEQUACIES IN THE SYSTEM DEVELOPMENT METHODOLOGY

A sound IT system development methodology should, *inter alia*, ensure that:

∗ the objective and scope of the IT project are well defined to meet the business requirements of the organization.

∗ the various options available are evaluated before freezing the scope of the project.

∗ the systems requirements are well specified so that the developed system delivers the desired outputs.

∗ there should be adequate acceptance testing of the system before its implementation.

∗ the contracts with vendors, if any, are effectively managed to ensure timely delivery with desired specifications, besides safeguarding the financial interests of the organization.

Shortcomings in the system development methodology adopted for developing CTBS are discussed in the following paragraphs.

3.6.2 Failure to opt for a standard integrated billing software

A telephone revenue billing software which integrates the functions of the Commercial and TR wings would facilitate on-line updating of data, thereby making better use of IT in ensuring timely and accurate billing. Since all the applications would access the same database, unaddressed bills would be minimized and processing of ANs and disconnections would be expedited.

Audit, however, observed that CTD opted for a non-integrated package and thereby missed the opportunity of implementing DOTSOFT, an integrated software package for customer services and telephone revenue billing, standardized (October 1998) by the Department of Telecommunications (DoT) for implementation in all the units of DoT.

In order to have additional features not available in its existing billing system, such as on-line cash counters, deposit refund system, billing of leased circuits/I-Net and other value added services, CGM, CTD awarded (December 1998) the work of development and implementation of a new TR billing and accounting system to M/s Tata Infotech Limited (TIL) at a cost of Rs 53 lakh. Audit, however, observed that the billing system was to be a stand-alone one rather than an integrated package. CTD had not carried out any cost-benefit analysis to compare the advantages of developing a stand-alone package for telephone revenue billing vis-à-vis an integrated package. It was also noticed that DoT had not insisted upon the implementation of the integrated standardized DOTSOFT package in a major telecom district like CTD. The Management stated that a cost-benefit analysis had not been done since no norms for it had been prescribed by DoT. The reply is not tenable as a cost-benefit analysis should invariably be undertaken before implementation of any major project.

Implementation of a stand-alone billing package like CTBS hampered the efficient functioning of revenue realization of CTD as discussed below:

3.6.3   Unaddressed bills

Bills in CTBS are generated based on customer profiles in the master data and meter readings from telephone exchanges.   Wherever meter readings are recorded in the exchanges for telephone lines but the master data for these phone connections has not been created due to non-receipt of completed ANs, the billing system generates unaddressed bills for call charges without the consumer numbers, names and addresses of the customers. Generation of unaddressed bills not only entails the risk of leakage of revenue but also puts the customers to hardship due to steep arrear bills later. As per the instructions of BSNL, an unaddressed bill should be cleared within three billing cycles.
Audit observed that during the period April 2002 to March 2005, 26,198 unaddressed bills amounting to Rs 3.83 crore were generated, which remained unpaid as of August 2005. Further analysis of database revealed that there were 9,190 unaddressed bills valuing Rs 1.57 crore which were pending for more than three billing cycles.

On-line integration of the commercial and billing systems would have greatly helped in minimizing the generation of unaddressed bills as also in their clearance.

Audit also observed that during the same period, there were 4,583 unaddressed bills amounting to Rs 66.80 lakh, for which master details were available but the same had not been linked with the consumer numbers. It was observed that though a facility for automatic linking of unaddressed bills with consumer numbers was available in CTBS, it was not used. On this being pointed out the Management accepted the fact and replied that the facility was not implemented due to difficulties like raising of credits and debits after creation of the master data. The reply showed that the package was not designed to handle such functional requirements.

3.6.4   Delays in processing advice notes

As per the rules of the Company, ANs for new phone connections should be completed within 15 days from the dates of their issue and those for shifting of phone connections should be completed within 30 days of their issue. Audit observed that 83,921 ANs for new connections and 8,339 ANs for shifting had not been completed within the prescribed period during April 2002 to July 2005. Non-completion of these ANs within the prescribed period resulted in loss of potential revenue of Rs 5.49 crore[+]. An integrated billing package, through its on-line monitoring features, would have aided the Management in the tracking of ANs and identifying bottlenecks.

[+] Average revenue per telephone line x (Delay in days / 365)

3.6.5   Delay in disconnection of telephone connections

The Company instructed (February 2003) that telephone connections of defaulting customers should be disconnected on the 35th day after the issue of their bills. Any delay in disconnection entailed the risk of further accumulation of dues on account of charges for calls made after the prescribed dates for disconnection. It was seen in audit that the disconnection lists created in CTBS were being sent to the telephone exchanges through messengers. Scrutiny revealed that in 54,180 cases, bills amounting to Rs 23.75 crore were outstanding against defaulters, of which Rs.8.03 crore pertained to defaulters with three or more bills outstanding. Call charges appearing in these bills proved that the disconnections had not been effected in time. An integrated billing system functioning in a network environment would have facilitated timely disconnections by providing access terminals in the exchanges for online viewing of the disconnection lists.

The matter was referred to the Management in August 2005 and their reply was awaited.

3.6.6   Delay in implementation of the project

Effective contract management ensures that a project is completed within the scheduled period and with all the desired specifications. Commitments of both the Management and the contractor have to be identified and spelt out clearly in the agreement to ensure compliance.

The contract required TIL to complete the project in 69 weeks in four stages from the date of signing of the agreement (November 1999), i.e. by March 2001, as shown in Appendix-XVI. Audit observed that TIL did not fully complete all the stages and left out certain important items of work like leased circuit billing, I-NET billing and data conversion/validation of deposits. Audit also observed delays in completion of the stages ranged from 40 to 135 weeks. In terms of the agreement, liquidated damages (LD) were recoverable in case of delay. However, it was noticed that no LD was recovered from TIL.

The Management stated (August 2004) that LD had been waived as the delays were mainly due to reasons attributable to CTD such as delays in providing circuit billing data, data for verification, site availability, and connectivity as well as deputing officials for training. This showed that CTD had not been able to effectively carry out its commitments for the implementation of the contract with TIL.

3.6.7   Non-imposition of penalty for non-compliance of the terms and conditions of the contract.

The agreement with TIL for development and implementation of the billing software for CTD had specified that any penalty for delay in completion of work or for non-compliance with the terms and conditions of the contract was to be adjusted from the security deposit submitted by them. The payment terms of the agreement stipulated that before releasing payments for each phase of work the vendor's invoices should be certified by CTD for completion of all items envisaged in the contract.

It was observed in audit that no penalty was imposed on the vendor despite failure on their part to complete the work as envisaged in the contract. As per the agreement with the vendor, a testing report was to be submitted on completion of every stage of work, but it was seen that detailed checking of each and every specification contained in the System Requirement Specifications (SRS) was not done. Instead, simple completion certificates were relied upon for releasing the payments.

A post implementation review was carried out in March 2005 and the report of the certification committee pointed out many shortcomings in the system such as non provision of billing extra rent for Direct Inward Dialling (DID) facility, data down loading from certain type of exchanges, etc. Further, as the performance guarantee submitted by TIL towards security deposit was not renewed beyond March 2003, CTD could not recover any penalty for the incomplete work.

The Management stated that renewal of the Performance Bank Guarantee(PBG) beyond March 2003 was not insisted upon as TIL had completed all major works except circuit billing for which CTD was responsible. The reply is not tenable, as a valid PBG should have been retained till successful completion of all the stages and satisfactory acceptance testing.

3.6.8   Deficiency in System Requirement Specifications

Defining the SRS is one of the most important stages in the development of an IT system, as all the requirements have to be identified at this stage for inclusion in the system to be developed. Inadequate specifications may result in non-fulfillment of planned requirements as described below:

The SRS for CTBS required that the system should include billing of leased circuits and I-Net. Audit, however, observed that the billing of these services, which amounted to Rs 64.88 crore in 2004-2005, was being done outside CTBS. On this being pointed out, the Management stated that telephone numbers comprised 8 digits but circuit numbers had 13 digits and thus they were not being accepted by the system. The reply showed that scalability[2] options were not kept in mind before firming up the SRS for the leased circuit and I-Net Billing module.

Further, the Company has proposed to implement next generation state of art Call Detail Records (CDR) based Customer Care and Convergent billing system, along with plans for deployment of Centralized Integrated Billing System. The process for the same was started in 2002. Convergent billing based on CDR is expected to facilitate the Company to face new challenges due to competition by providing effective and efficient billing with countrywide intranet.

As would be seen from the above observations, the billing and revenue realization through CTBS suffered on account of it being a non-integrated

---

[2] Scalability- How well a solution to some problem will work when the size of the problem increases.

package and the deficiencies at various stages of its system development methodology.

Recommendations:

    ✍ **The Company should strive towards having a standard integrated billing software for all its circles. For the purpose, the process of switching over to Call Detail Records (CDR) based billing system initiated in 2002, should be expedited.**

    ✍ **Pending introduction of the CDR based billing system, CTD should attempt on-line integration of CTBS with the existing commercial application software like CANMAPS, FRS[*], etc, after proper cost-benefit analysis.**

    ✍ **The facility available in CTBS for linking of unaddressed bills and consumer numbers should be enabled immediately for minimizing unaddressed bills.**

    ✍ **CTD should enable online access of disconnection lists to its exchanges to ensure timely disconnections.**

    ✍ **CTD should incorporate billing of leased circuits and I-Net in CTBS**

    ✍ **The Company should issue instructions, clearly specifying the IT system development methodology to be adopted by its units. These instructions should invariably include detailed steps to be followed for stages like project initiation, user requirement specifications, system requirement specifications, system design and acceptance testing.**

3.7   INADEQUACIES IN IMPLEMENTATION OF THE SYSTEM

Implementation of an IT system should be a well-planned process to fully derive the envisaged benefits. CTD implemented CTBS through a parallel run. Audit observed the following deficiencies in implementation of the system:

3.7.1   Non-validation of deposits data

One of the most important considerations before CTD was to ensure that the data from the existing COBOL billing package was properly migrated to CTBS. As per the agreement, TIL was to convert and validate deposit data from the old system and migrate them into CTBS. Audit examination of the database revealed that deposit data of both pre and post CTBS period were kept under suspense as unconfirmed deposits.

Due to non-validation of deposit data in CTBS, the function of refunds had to be necessarily done outside the system.

---

[*] Fault Repair System

The Management stated that the deposits were being maintained under suspense till the refunds were made and that efforts were on to reconcile the deposits maintained at the zonal level with the centralized deposit details in CTBS.

3.7.2   Parallel Run

As per the agreement, TIL was to conduct parallel runs for two full billing cycles for telephone connections where bi-monthly bills are issued and for two consecutive months for other services like Public Call Offices (PCOs), Integrated Service Digital Network (ISDN), etc, which were billed on a monthly basis. Audit, however, observed that a parallel run was conducted (January 2002) for just one month for all the connections and not for complete billing cycles. The results of the parallel run were not documented. Adherence to the specified duration for parallel runs would have helped the Management in detecting and rectifying the inconsistencies in the functioning of the system.

Recommendations:

✐ **The Company should ensure that implementation plans of IT projects are well-defined and the results of implementation are well-documented to facilitate change management and business process re-engineering at later dates.**

✐ **CTD should urgently validate the deposit details available in CTBS.**

3.8   DEFICIENCIES IN THE FUNCTIONING OF THE SYSTEM

A computerized billing package should be designed to ensure that there are no deficiencies, which can impact billing and revenue realization. IT applications should have in-built controls for validation of data.   Further, procedures should be in place for dealing with transactions, which fail to meet the input requirements. Management should effectively monitor the information system to ensure its proper functioning and early detection and rectification of deficiencies. It was noticed that CTBS provided various tools in the form of data analysis, exception reports, etc for the Management to monitor the performance of various functions as also to optimize performance. However, it was observed that effective monitoring was lacking in the following areas of revenue billing and accounting.

3.8.1   Working telephone connections not billed

The calls recorded in a telephone exchange are downloaded to CTBS, and the billing system generates a bill for the relevant billing cycle. After the bill is generated, CTBS updates the master data with the meter reading and date, up to which the connection is billed. Such entries act as a control to ensure up to date billing of all connections.

A scrutiny in audit of the bills, meter readings and master data tables showed that CTBS had failed to generate bills for 143 telephone connections which

registered 14.65 lakh metered calls during January 2003 to March 2005 even though meter readings were available in it.

It was also observed that the system had not billed trunk calls valuing Rs.2.92 lakh and 2.37 lakh local calls of 199 ISDN child numbers[3] from July 2004. These charges, which were required to be billed against the parent numbers, were not billed.

The Management accepted the fact and stated that supplementary bills had been issued for the unbilled connections. Instances of non-billing by the system despite the availability of the required inputs raised doubts about the credibility of the system.

3.8.2   Non-billing of phonogram charges

It was observed (July 2005) that phonogram charges were not billed by CTBS, despite the availability of the required inputs and a module for their billing being available in the system.

The Management replied that phonograms valuing Rs 1,81,804 only were unbilled as on May 2005 and efforts were on to bill the unbilled phonogram charges. On further verification it was found that phonograms valuing Rs 14.37 lakh were unbilled (August 2005). The reply is thus not tenable.

3.8.3   Non-processing of rental rebates for faulty telephones

CTD keeps track of all its faulty telephone connections through its Fault Repair System. Details of telephone connections, which are faulty for seven days and above, are downloaded into CTBS and based on these data, the rent-processing module of CTBS calculates rent rebates for the respective numbers.

It was observed in audit that rebates were not processed by CTBS in respect of 3,507 telephone connections, which remained faulty for seven days and above, for which the data was received in CTBS during the period February 2002 to July 2005.

3.8.4   Non-billing of service tax from non-exempted subscribers

Service tax on telephone bills is chargeable from all subscribers except certain exempted categories of subscribers notified by the Central Excise department from time to time.

Audit scrutiny revealed that service tax amounting to Rs 9.14 lakh for different months in respect of 8,823 bills was not levied on non-exempted subscribers during the period April 2002 to July 2005. The Management replied that service tax was levied in all cases by the system and there was no short claim. The reply of the Management is not tenable, as service tax was not claimed in the above cases as revealed through database examination.

---

[3] ISDN child numbers – Secondary numbers of the main (parent) number.

3.8.5 Discrepancies between Management Information Systems and actual telephone connections billed

Telephone bills are issued fortnightly, monthly or bimonthly on the basis of the type of connections. In the case of bimonthly billing, bills are issued by dividing the numbers into two groups of odd and even months. A bill should therefore, be generated for all connections at least once in two months. A check of the number of connections working at the end of a month and the number of connections billed in the subsequent bimonthly period provides a control to monitor whether all the telephones are being billed.

A comparison of the number of connections billed in the two month period of April and May 2005 as per CTBS with the working connections shown as per the Management Information Systems (MIS) report of CTD for March 2005 revealed that against 10.02 lakh working connections, 9.38 lakh connections were billed during these two months, leaving 64,000 connections unbilled. The SRS for CTBS envisaged generation of an MIS report containing details of equipped capacity, working numbers etc. but this feature was not available in the software which resulted in inadequate reconciliation between working lines as shown in the MIS and billed lines.

3.8.6 Inadequate validation checks

Adequate validation checks are necessary to ensure that only complete and valid inputs are accepted by the system so that data integrity is maintained and the output generated is reliable. Absence of adequate validation checks entails manual intervention which may lead to errors. The system should generate exception reports to identify transactions or data that are inconsistent.

A test check in audit revealed the following cases of data integrity violations due to inadequate validation checks in the system:

* Telephone connections provided one month after the date of application are entitled to interest on the initial deposit, to be adjusted as credit in the first bill. In 899 cases, CTBS generated credit vouchers for Rs.0.35 lakh erroneously though the connections were provided within one month of payment of the deposit.

* dates of completion of transactions were beyond the system dates. In such cases, the 'date field' could not be utilised for the purpose of billing and accounting.

* the end dates of the billing package option to be exercised by the customer on the basis of which bills were to be processed were earlier than the start dates.

* rental concessions to educational institutions were provided beyond the prescribed limits.

Recommendations:

☞ **CTD should examine the reasons for non-billing of telephone connections in spite of availability of the required inputs, and rectify the deficiencies.**

☞ **CTBS should be re-engineered for more effective validation checks to ensure data integrity and introduction of exception reporting mechanism.**

3.9 DEFICIENCIES IN INFORMATION TECHNOLOGY SECURITY

Information systems play a vital role in an organization's business operations and the achievement of its business objectives. For a computerized system to work efficiently and effectively, IT security policy and controls should be formulated and implemented. Observations on the IT security policy and controls of CTBS are detailed below.

3.9.1   Lack of comprehensive IT Security policy

The Company operates in a technology dependent environment which is IT driven. CTBS, being the billing system of an important unit of the Company unit, handles a large customer database with huge revenue implications, which calls for a properly documented IT security policy and procedure. However, the Company has framed no such policy which, *inter alia*, covered threats from viruses, tampering of customer data, network access threats and compliance requirements. The security procedures should be made available to all employees responsible for IT security.

3.9.2   Weak access controls

The orders (July 2001) of DoT as adopted by the Company, stipulated that passwords should have a minimum of eight characters and be a combination of upper and lower case alphabets, numerals and special characters. The CTBS system accepted password compositions of alpha numeric and special characters with a minimum length of four characters, which was in violation of the security instructions.

3.9.3   Use of generic user-id in transactions

Audit scrutiny of the CTBS database revealed that all users were accessing the database with a common user-id and all types of critical transactions were being done under this common user-id. For instance, it was observed that out of 21,786 cases valued at Rs 10.16 crore where refunds for excess payment by customers were authorised during the period April 2002 to March 2005, 15,216 cases valued at Rs.8.52 crore were authorised through the common user-id instead of through individual user-ids. Accessing and processing the database using a common user-id could lead to difficulties in fixing responsibility for errors/omissions and could give unnecessary scope for manipulation, unauthorized access and breach of system integrity.

3.9.4   Inadequate logging

Audit observed that though logs were available to capture the identity of users who carried out changes to critical data like tariff rates, bills, meter readings, etc., these logs were not effective as no transactions pertaining to tariff changes, status changes of customers, deletion and updating of data in various

tables, changes to the user master, meter reading and bills were captured in the log files.

It was further observed that

- ✍ The tariff change log table had not captured tariff changes that came into effect after the commissioning of CTBS. Telephone tariffs were changed in May 2003, October 2004, etc. The relevant log tables did not have fields to capture user-ids and dates of entry.

- ✍ the billing package options exercised by the subscribers were stored in a table. Although this data was crucial for determination of the tariffs applicable to consumers, user-ids and entry dates had not been captured in the case of 3.02 lakh records out of the 3.36 lakh records in this table.

3.9.5 Lack of segregation of duties

One of the methods to ensure that transactions are properly authorized and recorded, is effective segregation of duties. Even if the IT department consists of few personnel, compensating controls must exist in order to mitigate the risks resulting from a lack of segregation of duties.

In an RDBMS and a multi-user operating system environment, the database function should be monitored by a Database Administrator (DBA) who should have access to the database tables and be responsible for ensuring the integrity of the data. The System Administrator (SA) should be responsible for checking the log files pertaining to the system access. It was observed that the CTBS database had more than 200 data tables, which formed the core data for collection of revenue from basic services, but the same person was performing the duties of both the DBA and the SA.

The matter was referred (August 2005) to the Management and their reply was awaited.

3.9.6 Business Continuity Plan

The objectives of preparing a business continuity and disaster recovery plan and associated controls are to ensure that the Management is able to process, retrieve and protect the information maintained in the system in the event of an interruption or disaster leading to temporary or partial loss of computer facilities. No documented business continuity and disaster recovery plan had, however, been formulated by CTD. There was no offsite storage of backup data, which was being stored in the same premises.

The Chief General Manager, CTD appointed (July 2004) M/s. S.B.Billimoria & Co., Chennai at a cost of Rs.1.95 lakh to conduct a review of CTBS applications and general computer controls.   The major observations included in the report (November 2004) of the consultant were that CTD should formulate and implement a security policy, a business continuity plan and a disaster recovery plan. The Management stated (August 2005) that these were being implemented in a phased manner. However, its implementation had not been started till September 2005.

3.9.7 Inadequate alternative arrangements for personnel to meet contingencies.

Availability of trained personnel is a vital requirement for smooth functioning of an IT system. The billing centre of CTD was manned by officials of the level of Chief Accounts Officers, Senior Accounts Officers, Assistant Accounts Officers and Junior Telecom Officers of CTD who had been trained to handle the systems including system administration and database administration. Audit observed that there was no documented procedure for handing over of DBA passwords, the system duties to be performed by the incumbent in contingent situations such as non-availability of key personnel like DBA/SA due to leave, promotion or transfer.

Recommendations:

✄ **CTD should formulate and implement an IT security policy and review it periodically.**

✄ **Logical access controls of CTBS should be strengthened by adequate logging of changes to critical data like master data, meter readings, etc. The audit trail function should be activated.**

✄ **CTD should ensure proper segregation of duties between the Data Base Administrator and the System Administrator**.

✄ **CTD should maintain an offsite storage location for backup data.**

✄ **CTD should formulate policies for anti virus, data backup and prepare a 'Business Continuity Plan' and 'Disaster Recovery Plan', for early implementation.**

✄ **CTD should prepare a plan for alternate arrangements for personnel in contingent situations.**

3.10 Conclusion

The efforts of CTD in replacing the COBOL billing package with CTBS though sincere, suffered from non-adoption of systematic procedures like IT system development methodology and deficiencies in implementation, internal controls, monitoring mechanism, IT security and human resources management as brought out in the report. The billing deficiencies as brought out point to existence of revenue leakages. An effective revenue assurance mechanism could help the Management in plugging these revenue leakages emanating from manipulation of billing databases, billing errors, inefficient collection and detecting frauds and ensure the completeness of revenue generation and collection. This would have a positive impact on the functional and operational efficiency of CTD. Switching over to a uniform CDR based billing system; issuing of detailed instructions on system development methodology and implementation; strengthening of internal controls, the monitoring mechanism and IT security controls and introduction of a revenue assurance mechanism should assist CTD and the Company in achieving greater effectiveness and efficiency in billing and revenue realization as also in IT project management.