

**FINANCE DEPARTMENT**

**3.6 Computerisation of Treasuries in Karnataka-‘Khajane’**

**Highlights**

*The project ‘Khajane’ was implemented with the aim of providing Drawing and Disbursing Officers, Controlling Officers and Chief Controlling Officers the details of expenditure for the purpose of reconciliation, restricting payments at the treasuries to budget allocations, ascertaining the Ways and Means position of Government, etc. The Project was implemented without the preparation of a comprehensive user requirement specification leading to deficiencies in Information Technology operations and controls. Codal provisions for awarding the contracts for establishing network connectivity were also not followed.*

Codal provisions were ignored while awarding the contract for establishing network connectivity.

(Paragraphs: 3.6.4.1 & 3.6.4.2)

The System was not able to take care of the relevant rules for adjustments of NDC bills against AC bills.

(Paragraph: 3.6.6.1)

The System was ineffective in ensuring correctness of payments made to the Housing Development Finance Corporation.

(Paragraph: 3.6.6.3)

The System either did not have proper input validations or these validations were bypassed resulting in violation of various financial and service rules.

(Paragraph: 3.6.7.2)

The System did not facilitate uploading of budget related data from the Finance Department Package.

(Paragraph: 3.6.8.3)

Inadequate security arrangement exposed the IT assets and data to risk of damage/misuse, while change control procedures were inadequate.

(Paragraphs: 3.6.9.1 & 3.6.9.2)

The back up data was not stored off-site which may lead to avoidable loss of data in case of crashes.

(Paragraph: 3.6.9.4)

### 3.6.1 Introduction

The Department of Treasuries headed by the Director handles all cash transactions of the Government. The receipt and payment transactions are carried out through 31 District Treasuries and 184 Sub-treasuries spread over the State. On the recommendations of an Official Committee appointed in August 1997, the Government ordered (July 1999) implementation of the project ‘Khajane’ with the main objective of providing details of expenditure to Drawing and Disbursing Officers (DDOs)/Controlling Officers (COs)/Chief Controlling Officers (CCOs) for the purpose of reconciliation, facilitating Treasury Officers to restrict the payments to the budget allocations of DDOs/COs/CCOs, making available Treasury Transfer Receipts reports required by various Government departments, assisting dynamic reallocation of budget allotments and to ascertain the Ways and Means position of the Government on any day. The implementation of project commenced (January 2001) after a tripartite agreement was signed between the Director of Treasuries (DoT), Software Technology Parks of India (STPI) (Network Provider) and CMC Ltd (CMC) (System Provider). A Wide Area Network (WAN) was set up by STPI, at a cost of Rs.14.23 crore, using VSAT terminals at all the 216 locations to a central database server at Bangalore and recurring maintenance cost of Rs.2.90 crore per annum. CMC developed the application package at a cost of Rs.17.11 crore which included supply/installation of hardware, software and facilities required for running the application package at each location and maintenance of the systems for five years at a cost of Rs.6.28 crore. Rs.46.53 crore has so far been spent (September 2006) on acquisition, implementation and maintenance of the system.

### 3.6.2 Organisational set-up

The Department of Treasuries is headed by the Director of Treasuries. The Treasury Network Management Centre (TNMC) at Bangalore which controls the central server “KUBERA” and the hub of the KHAJANE-net is headed by a Deputy Director of Treasuries and 23 support staff. All District Treasuries, headed by District Treasury Officers (DTO), are provided with high-end server with UNIXWARE operating system and client systems ranging between 5 and 25. The sub-treasuries, headed by Sub-Treasury Officers (STO) render monthly accounts online to respective DTOs following up with vouchers and other documents.

### 3.6.3 Scope and methodology of audit

The audit was conducted to evaluate the efficiency and effectiveness of the system in achieving the stated objectives and to assess the adequacy of good practices of Information Technology (IT) governance along with controls built in to ensure data integrity, security of data, systems and other IT assets. A test-check of records maintained electronically and manually was conducted in

the office of the DoT, TNMC, six<sup>24</sup> District Treasuries and three<sup>25</sup> Sub-treasuries. The records relating to treasury transactions in some of the offices of CCOs, COs, DDOs were also test-checked between October 2005 and February 2006. The sample data of the information contained in data tables received from TNMC in the form of an Export Dump was scrutinised using the generalised audit software – IDEA<sup>26</sup> and SQL<sup>27</sup>. The audit findings are detailed in the succeeding paragraphs:

### **3.6.4 Project Management**

#### **3.6.4.1 Award of contracts for establishing network connectivity on limited tender basis**

**Discrepancies in payments and award of contracts led to avoidable expenditure and deprived the department the advantage of competitive rates**

According to Karnataka Public Works Department (KPWD) Code, where the value of contract exceeded Rs.two crore, tenders were to be called for through advertisements in news papers. While the development and maintenance of the application package (cost: Rs.23 crore) was made after calling for bids from a limited number of firms, the work of establishing the WAN costing Rs.15 crore was entrusted to STPI on an on-cost basis without calling for tenders. Similarly, the work of cabling, electrification (Rs.1.22 crore) and providing services of security personnel was entrusted to STPI without availing the benefit of competitive rates.

The Department stated that STPI was a Government of India concern and that all the procurements had been done with the approval of the Committee formed for the purpose.

The fact remained that the Department did not avail the benefit of competitive rates by giving wide publicity in the news papers for larger participation of the intending bidders in the tendering process. The reply was also not tenable as STPI in turn hired the services of HCL-Comnet for setting up the network at a cost of Rs.12 crore and list of bidders for the work included companies which had participated in the tendering process for development of the application package.

#### **3.6.4.2 Evaluation of bids**

It was noticed that limited tenders were invited for development of the application package (including hardware and networking) out of the list of Total Solution Providers maintained by the Government. In view of the size and significance of the project, the Department could have obtained more competitive rates with wider publicity and by negotiating with the first two lowest bidders (HCL Info Systems and NIIT), instead of entrusting the work to CMC which was the third lowest bidder. Moreover, KPWD Code stipulated that in cases where recourse to invitation for fresh tenders could not be taken

---

<sup>24</sup> Bangalore (Rural), Bangalore (Urban), State Huzur Treasury-Bangalore, Pension Payment Treasury- Bangalore, Mandya & Tumkur

<sup>25</sup> Doddaballapura, Hoskote and Magadi

<sup>26</sup> Interactive Data Extraction and Analysis

<sup>27</sup> Structured Query Language

due to there being no prospects of getting lower favourable rates, negotiations had to be conducted by the competent authority, only with the lowest bidder. However, the rate of CMC was accepted without terms and conditions being agreed to. The offer was made at Rs.17.11 crore for the system development which included supply and installation of hardware (including local networking in each location), and training of 600 personnel in the usage of application software. No break up for various components of the system development was specified.

The Department stated that the financial evaluation of the bids was against one value quoted for all items to be supplied and hence break up was not incorporated. It further stated that as the original rate quoted by CMC and the rate at which signed by them were entirely different, they were given an opportunity to rework their break up which was approved by Government and payments were made as proposed by CMC.

It was noticed that while cost of uninterrupted power supply system (UPS) offered by HCL Info Systems (Lowest) was negotiated and brought down by Rupees one crore, after comparing with offers of NIIT and CMC, no negotiations were held with CMC. Consequently, payments were made at higher rates than those of HCL Info Systems (L1) resulting in extra payment of Rs.2.03 crore, as detailed below:

**Table 1: Comparison of offers**

(In rupees)

Component	Rate quoted by HCL(L1)	Rate at which payment made to CMC	Difference	Quantity	Total payment
District Server	2,39,972	2,89,720	49,748	30	14,92,440
SHT Server	3,85,997	4,63,561	77,564	1	77,564
Desktops	49,737	51,257	1,520	447	6,79,440
Dot-matrix printer	10,536	10,700	164	262	42,968
Application S/W	81,17,500	2,41,61,093	1,60,43,593	1	1,60,43,593
Networking	14,72,051	33,98,502	19,26,451	1	19,26,451
<b>Grand total</b>					<b>2,02,62,456</b>

It was also seen that under the tripartite agreement, 10 per cent of the contract value was to be paid only after successful pilot testing. Contrary to this, CMC was paid an advance of Rs.1.80 crore for purchase of hardware for pilot sites. The Department stated that the advance payment was in view of the good progress achieved.

It was further noticed that technical specifications as listed out in the tripartite agreement were at variance with those as per invitation to bid as specifications for UPS were not clear in the invitation to bid. Both HCL Info Systems and CMC had quoted the costlier Sealed Maintenance Free (SMF) batteries but in the tripartite agreement, it was changed to cheaper tubular batteries. Further, the bid document required supply of anti-virus software but it was not

included in the agreement for which Rs.11 lakh were paid subsequently. The type of cabling for local networks was also not clearly spelt out in the invitation to bid and was changed to five times costlier rate subsequently.

Thus, there was an avoidable payment of Rs.2.14 crore and also unintended benefits to the vendor due to award of contract without negotiating on the rates for individual items; not insisting upon SMF batteries or obtaining discounts for supply of cheaper batteries; advance payment in contravention of the terms of the agreement; and change of specifications while executing the agreement.

#### **3.6.4.3 Avoidable expenditure on additional functionalities**

In 2003, CMC submitted a proposal for 25 additional activities and quoted Rs.39.09 lakh for their study, design and development. It was noticed that many of these activities were either already contemplated in the procedure manual issued to vendors or were discussed in the Software Requirement Specification (SRS) document which was proposed by CMC and approved as final before the pilot study. Had the SRS been finalised after pilot study, extra payment could have been avoided.

#### **3.6.4.4 System maintenance**

The contract value for Facility Management Services (FMS) payable to CMC was fixed at Rs.6.28 crore payable in 20 equal instalments of Rs.31.40 lakh at the end of each quarter. The maximum response and restoration time for the FMS was one day after the faults were reported. Penalty was to be calculated based on delay in response beyond the maximum limits mentioned and deducted from maintenance bills. As the quantum of delays was very high, the percentage deduction to be made worked out to almost 100 *per cent*. However, agreement restricted the penalty to five *per cent* only.

It was noticed that some of the problems relating to maintenance of software and hardware which kept recurring month after month were end of day problems, cheque printing problems, difficulties in the generation of reports and problems in closing of monthly accounts. The department stated that only unique problems have to be considered out of the total number of problems reported; problem reporting was not the major component of FMS; the vendor had been penalised wherever there were inordinate delays; and the help desk activity was badly affected due to high attrition rate during 2004-05.

The reply is not relevant since the problems reported affected the functioning of the system resulting in problems in closing of monthly accounts.

### **3.6.5 System Development**

It was noticed that a structured system development approach was not adopted in executing the project as no project initiation document was prepared and no feasibility study was carried out by drawing up of a report indicating the

Delayed response time in clearing the faults indicated that the faults needed to be studied and appropriate action to be taken to address the root cause of the problems

alternative solutions. A User Requirement Specification (URS) document was not brought out clearly defining the scope of the system, key features that should be included and reports to be generated. This resulted in a number of design deficiencies which adversely affected the functioning of the system (Paragraph 3.6.6).

The Department stated that when the project was conceived, use of IT in government departments was not much, and further that no standards were prescribed, no road maps were available and there were no precedents to follow. It added that 'Khajane' being a path-breaking project, not many of the standard practices were strictly followed and hence status documents like resources used, milestones achieved and road map, feasibility study, cost-benefit analysis were not done exactly according to the norms.

The reply is not acceptable, as the services of the experts were already available with the Department and moreover best practices for IT system acquisition and implementation were available and should have been referred to.

### 3.6.6 System Design

#### 3.6.6.1 *Improper development of the system for monitoring receipt of detailed contingent bills against abstract contingent bills*

**Non-inclusion of appropriate controls in the application system and lack of circular instructions to DDOs rendered huge sums drawn on AC bills without details of expenditure**

Test-check of the database of district treasuries for AC Bills drawn/NDC Bills submitted revealed that in three Treasuries NDC Bills were not submitted or the fact of submission not noted against AC Bills drawn by various DDOs during the period 2002-03 to 2005-06 (up to January 2006) in 3,128 cases involving Rs.517.50 crore.

Under the Manual of Contingent Expenditure, a DDO was permitted to draw only up to Rs.500 without special sanction of the controlling officer. An analysis of the database indicated that in 516 cases, the maximum amount was recorded as more than Rs.500, ranged from Rs.600 to Rs.25 lakh. This exposed the system to the risk of misuse and avoidable irregularities. The Department stated that data would be verified and necessary corrections carried out.

The NDC bills submitted to treasuries were not noted in many cases against the corresponding AC Bills drawn. Though objection was raised by the system for the previous bill irrespective of the fact whether submission of NDC bill was due or not, objections were being overruled and further AC bills passed. There was no provision for stoppage of further AC bills whenever NDC bill due was not submitted.

Thus, the system developed could not take care of the requirements of the Rules and Government Orders for effective monitoring of the submission of details of expenditure for amounts drawn on AC bills leading to non-accounting of moneys drawn from treasuries.

The Department stated that the software to cater to the needs of accepting NDC bills was under development and would be implemented from 2006-07.

### 3.6.6.2 Classification of transactions

Audit noticed a number of misclassifications which indicated the deficiencies in design and development of the package leading to inaccurate accounts and overstatement/understatement of receipts/expenditure.

A few examples are given below:

**Absence of key controls in the application package resulted in many misclassifications that made the system less dependable as also affected the true and fair nature of accounts**

- ⌵ Though the data entry was made as ‘building expenses’, and ‘general expenses’, the reports printed for the period between July 2005 to November 2005, involving an amount of Rs.57.94 lakh in 25 cases, depicted the same as ‘other charges’ and ‘other office expenditure’. It was stated that the system discrepancy had since been rectified.
- ⌵ The commercial tax receipts remitted in banks other than State Bank of Mysore (SBM) were accounted for by a treasury on a single challan furnished by SBM to the treasury.
- ⌵ In nine cases involving Rs.215.82 crores, transactions under deposit accounts were classified under incorrect heads of account.
- ⌵ The data table of the classified accounts of a treasury showed that object head field was blank in 25,610 cases for the period from April 2004 to December 2005 involving an expenditure of Rs.254.72 crores. The absence of the detailed head to which these payments related, rendered the accounts already booked, inaccurate. The Department stated that in case of deposit transactions there would be no detailed heads. The reply is not tenable since all the cases cited were not deposit transactions but also included heads of account like land revenue, interest payments, pensions.

### 3.6.6.3 Non-generation of details required for Housing Development Finance Corporation (HDFC) payments

**Absence of provision to support and determine dues of HDFC resulted in huge sums of money being paid unverified**

Payments made to HDFC relating to house building loans to Government servants during 2003-04, 2004-05 and 2005-06 were Rs.28.75 crore, Rs.22.26 crore and Rs.15.04 crore (up to November 2005) respectively. It was noticed that the system did not support generating a report for the total amount payable to HDFC every month detailing amounts due towards principal and interest, subsidy *etc.* As such, the demand raised by HDFC was paid without ensuring the correctness of the claim considering the rate of interest, type of loan, *etc.*, that varied from year to year. The Department replied that, as all this exercise would not have resulted in complete elimination of manual incorporation in the ledgers, it was decided to get comprehensive software developed for the purpose of accounting HDFC deductions. The reply is not acceptable as the package did not support verification of the monthly demands of HDFC by correlating them with recoveries from salaries which were available in the system.

#### 3.6.6.4 Pension related module

Audit noticed multiple design deficiencies in the pension related module which are detailed as follows:

In the “Pension Module” pension field accepted entry of amounts without minimum and maximum limits. Negative figures were found in some cases for basic pension. Total pension amount did not match the break up details in a few cases. The commuted value could not be restricted to the prescribed limit of one-third of the pension. Many essential fields like sanction order number could be skipped as they were not mandatory. Gross service could be entered as ‘nil’ or 50 years. Net service values could not be separately entered. There was no provision for watching receipt of life certificate of social security pensioners.

The forwarding letter to the bank was not generated correctly by the system, as for example, the name of the Bank and branch did not appear; instead of the total commutation amount, the basic pension amount was shown; the symbol “<” appeared in place of reduced pension amount and the amount of family pension was not displayed.

**Lacunae in the system that may lead to risk of misuse**

Once a Pension Payment Order (PPO) was generated, changes to verify the mistakes in data entry in the pension module could not be carried out. Corrections were, therefore, made in manual records. In the alternative, the IDs were suspended/closed and fresh IDs created. As the suspended IDs could be revived, this exposed the system to the risk of misuse/irregularities. It was noticed that in one case, payments were made to the same person in two new PPO IDs. Although two Old Age Pension (OAP)-PPO IDs were suspended in a treasury, payments continued to be made. The Department stated that all such cases would be reviewed and excess amount, if any, would be recovered.

In a few cases enhanced family pension was continued to be paid even after due dates for restoration. In a few cases gross amounts did not tally with the break up values of payments, net amount and pay order amount did not tally, which indicated lack of appropriate controls which may lead to incorrect reports. The Department stated that the discrepancies would be looked into.

#### 3.6.6.5 Other deficiencies

Specimen signatures of DDOs did not pop-up for compulsory check for authenticating bills presented for payment. It could be viewed only if the user chose to do so. Bills could be passed without such verification. An analysis of the table containing DDO details for each treasury revealed that a system-generated number was given to the signature of each DDO captured by scanning his specimen signature. It was found that instead of a unique number assigned for each DDO, there were 1,821 active records, which had the same GDDO code (00001). This indicated that there was a lacuna in the generation of GDDO codes. Similarly, there were 14,830 cases with a GDDO code of ‘99999’.



### **3.6.7 Application control**

Application controls are case specific and have a direct impact on the processing of individual transactions. These controls are used to provide assurance that all transactions are valid, authorised, complete and recorded. Audit noticed the following deficiencies in application controls.

#### **3.6.7.1 Input control**

To ensure that correct and relevant data is entered into the system to generate reliable output, a combination of controls over the input of data facilitated by proper validation checks in the system is essential. However, due to deficient input controls and insufficient validation checks, there were numerous instances of incorrect data being stored and processed by the system.

#### **3.6.7.2 Ineffective validations provided**

Validations that are provided to ensure compliance with financial and service rules, were not mandatory. Even if the user opened validation screen, options were to be ticked by exception and the user was not required to confirm each validation. Frequently occurring deficiencies in the bills could not be added by the user. As there was no compulsory sequence for various menus/screens to be navigated, various validations provided were ineffective.

The fields to record the dates of Government Order or the date of authorisation by the Accountant General (AG) for creating a DDO, accepted any future date as well. There were 1304 and 970 records of dates for Government orders and authorisation of the AG respectively that contained dates beyond the year 2050. Similarly, it was found that different designation descriptions were entered for the same DDO.

In one department, the head of the department addressed the Treasury Officers pointing out that the expenditure in district offices was wrongly shown as incurred by their Directorate at Bangalore. The treasury department replied to an audit query that misclassifications could be due to incorrect data provided by the DDOs. The reply is not tenable as the system should not have accepted bills against the head of account of the directorate from a district level officer.

There were instances where the detailed head-wise compiled accounts displayed zero in the amount column even though the related Abstract of Schedule of Payments indicated substantial sums as paid.

The inaccurate entries indicated lack of proper input validation controls or that controls in place could be bypassed. It also indicated that suitable monitoring mechanism was not in place to the review entries.

**Lack of appropriate input controls rendered the system incomplete due to errors in data capture**

### 3.6.7.3 Data entry

Lack of data capture controls led to many avoidable misclassifications and also affected the true and fair nature of accounts and MIS reports

It was noticed that during September 2003, receipts pertaining to Defence Department were booked twice by the State Bank of Mysore, Shivajinagar Branch, Bangalore, went undetected during the data capture at the treasury level resulting in an excess accounting of Rs.48,00,263. This was yet to be rectified in accounts and also necessary corrections to the database effected.

Modifications to mode of payment of pensions were not put through screens meant for the purpose but were being managed by suspending or closing the old IDs and opening new ones in their place. As the suspended IDs could also be revived, the procedure followed exposed the system to risk of irregularities as also the extent of modifications made could not be monitored.

The system did not support prompting incorrect entries made as deductions towards House Building Advances though it related the payments towards HDFC loans and *vice versa*. Similarly, incorrect entries of Motor Cycle Advances - principal and interest were not prompted by the system. Misclassification due to ineffective prompt by the system or lack of second level checks resulted in adverse balances under various loan heads of account, as in nine cases, misclassifications were observed involving Rs.8.78 lakh. The Department stated that the system could prevent misclassification into HDFC only and not the other way. The reply is not tenable as the system needed controls eliminating misclassifications of HDFC recoveries into HBA which resulted in adverse balances.

The above mentioned discrepancies indicated lack of proper input validations in the package and ineffective second level check of data entry with regard to the classification/capture of essential data. Action is to be taken to increase the awareness among the data entry operators and DDOs to facilitate capture of essential data and also to classify the transactions correctly to make the system more effective.

## 3.6.8 IT Operations

### 3.6.8.1 Generation of department-wise recovery particulars

Absence of important feature to generate department-wise recovery particulars

Except SHT, Bangalore, none of the treasuries furnished department-wise abstract of provident fund recoveries duly tallying with overall totals of all sub-treasuries along with the figures of the district treasury. Further, in many cases, key information like full name, designation, relevant account number were either not captured in the system or ensured that they were available in the schedules at the time of passing the bills, indicating insufficient input controls and non-provision of an essential feature in the package.

### 3.6.8.2 *Deposit accounts module*

Lack of appropriate output controls rendered certain reports unreliable

Article 286A of Karnataka Financial Code requires that a Personal Deposit account created by debit to the Consolidated Fund should be closed at the end of each year and a fresh account opened with a nil balance in the succeeding year. The system did not have any provision for such closure of accounts.

In one treasury, the savings bank account sub-module did not work. Consequently, transactions of all such savings bank accounts were being manually processed and cheques written by hand. The lacuna in the system needs to be addressed to bring all transactions online.

Summary of transactions of a set of deposit accounts were reported to AG (A&E) through a plus and minus memorandum. The system could not, however, generate reports in respect of revenue deposits and lapsed deposits. The totals of the various columns therein were not depicted in the reports so generated. The reports would not be completely useful without the totals of each column. The lacunae made the system less user-friendly.

### 3.6.8.3 *Inadequate controls in uploading budget allocations*

Absence of certain controls in uploading the budget allocations exposed the system to risk of irregularities

Though the Finance Department (FD) had the connectivity to the network, the treasury package did not support data interchange with budget modules of FD package. A user-friendly procedure could have obviated manual intervention for conversion of data, which was currently not authenticated by any Officer from FD. The Department stated that the authentication would be obtained in future. Audit noticed that there were many cases of expenditure booked without budget provision indicating lack of key controls.

Other cases of discrepancies noticed are as follows:

- ✎ The specimen signatures of the CCOs were not properly recorded in the files/ system. The letters intimating allotments were not signed by CCOs. Corrections to the data were carried out by Officers in TNMC but not got confirmed by from CCOs. Cuts and redistributions in allocation were carried out on 'Problem Reports', without any written documentation from CCOs. Database contained details of 23 officers in the DDO list of a department though they did not belong to that department. As the budget allocations were made by the head of the department among his DDOs, the system was exposed to risk of misuse of budget allocation by DDOs outside their department.
- ✎ There was no second level check for this item of work that involved allocation of funds. The Department stated that the second level check would be introduced and action taken to avoid the discrepancy pointed out.
- ✎ In respect of uploading of allocations to DDOs in the treasuries, the allocations were brought in floppies by the COs and the same was uploaded by making corrections wherever found necessary. However, the package did not support keeping an audit trail of changes made by persons

other than the competent authority. The uploading done in treasuries was also not being subjected to second check.

These discrepancies indicated lacunae in the procedures that exposed the system to risk of avoidable irregularities.

#### 3.6.8.4 Maintenance of Local Masters

In the test-checked treasuries, the records from which the local masters were created were not made available. Database of pensioners existing prior to computerisation had not yet been completely created. Correctness and completeness of the data capture could not, therefore, be verified in audit. Non-availability of such records rendered rebuilding of masters difficult. It also affected the clarification of problems and settlement of claims.

### 3.6.9 General controls

General controls create the environment in which IT applications and related controls operate. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications *i.e.* application controls. Audit noticed a number of deficiencies in general controls which are detailed below:

#### 3.6.9.1 Security of systems, data and other IT assets

**Inadequate security arrangements exposed the system to risk of damage to IT assets and misuse of systems**

Server room was not kept under lock and key in the test-checked treasuries. Line printers/ computer systems were installed in the server room and printing activities were carried on. No circular instructions regarding maintenance of server room were made available in the treasuries test-checked. A log book for monitoring the activities of server operations, its security, problems of facilities and speed of the network *etc.*, was not maintained or was not up to date in the treasuries test-checked as required according to a circular from the Directorate.

There was no fire fighting equipment in/around the server room in many treasuries and the air conditioners were out of order in some locations. No systematic record was maintained regarding periodical maintenance/on call details in respect of hardware, V-SAT, UPS, Printers, *etc.* Protecting the server room and other IT assets against possible physical damage or unauthorised access needed to be considered and appropriate instructions issued.

No documents had been maintained at TNMC to indicate conducting of periodic and ongoing review of access profiles, unsuccessful log-ins *etc.*; fire, weather, electrical warning and alarm procedures; air conditioning, ventilation, humidity control procedures; security breach alarm process; security awareness and training programs for the TNMC as well as for the treasury organisation as a whole; need for periodical change in security service

agencies; penetration test procedures and results; health, safety and environmental parameters for follow-up; staff facilities, rotates of shifts and appropriate holidays and vacation both for treasuries' staff and the vendors' staff; and environment aspects like procedure for disposal of e-waste. It could not be ascertained whether they were working at satisfactory levels. It was stated that these issues would be considered in consultation with the competent authorities.

In some of the treasuries test-checked, there was no mechanism to monitor the unsuccessful log-ins by unauthorised persons. Many users in various counters were leaving the system open and there was no mechanism for automatic log-off which rendered the system exposed to risk of unauthorised use. No written instructions were issued regarding change of passwords periodically and structure of passwords.

The System Administrator role was assigned to officials other than Treasury Officers in many cases. It was also observed that certain users were able to perform transactions in spite of their IDs being de-activated. There were instances where the same person worked as data entry operator, Assistant Treasury Officer, Treasury Officer and System Administrator while passing bills. Lack of clear segregation of duties and controls on user-IDs exposed the system to risk of irregularities. The Department stated that suitable instructions had been issued regarding assigning of role IDs and action was being taken to fix the bugs pointed out. No programmes to highlight the importance of security awareness had been arranged in any of the locations test-checked. Holding of such programmes to increase security awareness should be considered to avoid possible losses due to security lapses.

**Improper maintenance of stock accounts could lead to pilferage/misuse of IT assets**

The receipts of IT assets were not recorded in the stock accounts as and when they were received under proper attestation. Only a printed account in a bound volume of registers maintained at TNMC was made available to audit. No account of IT assets in stock was maintained at the treasuries. Assets relating to network (Rs.13 crore) were not found to have been taken to stock. 402 desktops only were taken to stock against 624 purchased. Similarly, against 218 servers (each costing Rs.2.90 lakh) purchased, 216 were recorded in stock. There was no record of movement of equipment for repair *etc.*, as no system of issue of gate passes was in practice. No record of annual verification of stock having been carried out in any of the years had been maintained. It was noticed that the line printers were out of order in some treasuries. Absence of proper mechanism to take the assets to stock and subjecting these to periodical physical verification exposed the assets to the risk of pilferage or misuse. It was stated that suitable instructions would be issued to all treasuries to carry out annual verification.

### 3.6.9.2 Change management controls

**Lack of systematic change management controls could not bring out orderly documentation of changes to system**

A number of changes to the ‘Khajane’ program had been carried out after it was installed in the year 2002. To minimise the likelihood of disruption, unauthorised alterations and errors getting into the application package, a management system which provided for the analysis, implementation and follow-up of all changes requested, was to be in place. However, no clear documents had been maintained in respect of request for change, specification of change, request to move source into test environment, completion of acceptance testing, request for compilation and move into production. Similarly, no documents were maintained to show that overall and specific security impact was determined and approved by a responsible designated officer of the Department.

The source code was not changed soon after the new tested program was replaced, even though copy of the source code was with the department. Regarding other issues, it was stated that suitable guidelines were issued (October 2006).

### 3.6.9.3 Inadequate training and supply of user manuals

**Lack of ongoing training system affected the efficiency of operations**

There was no policy for training of employees on an ongoing basis taking into account uneven distribution of trained personnel due to transfer, retirement, *etc.* Only one training programme was conducted since the package was implemented three years ago. No refresher courses had been conducted. It was noticed that sufficient copies of user manuals were not available. The manuals prepared in the beginning were yet to be revised though new version of the application package had been released as also many new forms and changes have been brought about in the application package. Though the vendor had to supply the system administrator manuals, it has not been made available. Action needs to be taken to provide sufficient number of user-friendly updated manuals for improving the efficiency of operations. The Department also stated that appropriate recruitment and training were being considered for smooth running of the project.

### 3.6.9.4 Off-site storage of back up data

**Inadequate arrangements for back up could lead to avoidable loss of data and time in case of crashes**

Back up of data was being taken at the end of each day in a weekly cycle and stored in the table-draw of a counter clerk in some of the test-checked treasuries. No instruction for storage of back up media, its location, off-site back up, *etc.*, was available in the treasuries test-checked. Difficulties were faced as no back up was taken in one sub-treasury where there was a server crash. As per the back up policy furnished there was no off-site back up of TNMC data other than back up at Disaster Recovery Centre (DRC), Dharwad. In case of connectivity failures and crashes in TNMC, data would not be available for recovery.

The Department, however, stated that back up of TNMC data was kept at the Directorate. Further, even though back up was taken on DAT cartridges no

mechanism was in place to record that the back up was actually taken and periodically tested independently for retrievability. Back up procedures needed to be reviewed for safe custody of the first copy in strong room/steel cupboards, considering storage of a second copy in off-site location as also a system for a regular check of the retrievability of the back up data.

#### **3.6.9.5 No mechanism for internal audit of systems**

No internal audit of IT Systems was being carried out periodically in any of the treasuries and TNMC. It was stated that this was being taken up. A continuous internal audit helps in proper maintenance of the systems, their efficiency and effectiveness and its security.

### **3.6.10 Conclusion**

The process of acquisition of hardware and software for the 'Khajane' project was not done following the best practices which facilitate transparency and efficiency in such projects. The project was implemented without the preparation of a comprehensive URS document resulting in non-provision of some of the key features in the application software like a proper system for monitoring submission of NDC bills; adequate support for HDFC dues; and providing department-wise recovery particulars in respect of GPF, *etc.* The controls and validations provided could be skipped and hence were not fully effective. The environment in which the entire system was being run was not satisfactory as inadequate security of IT assets as also data was noticed.

### **3.6.11 Recommendations**

- ✎ Appropriate controls and validations should be introduced to take care of accurate data inputs and outputs.
- ✎ System should support accounting of recoveries and repayments to HDFC.
- ✎ Appropriate change control procedures have to be adopted to make the changes to the system more orderly and with proper authority.
- ✎ The Government should come out with a comprehensive plan addressing the issue of security of IT assets which should be complemented by a proper disaster recovery plan to ensure continuity of operations in case of an adverse event.

**3.6.12** The above points were referred to Government in September 2006; reply had not been received (October 2006).