~~transfer price and manner of payment in consultation with MoR, and as of June 2015, the proceeds from transfer of equity remained un-realised from MoR. Meanwhile, the Balance Sheets of KMRCL, as on 31 March 2013 and 31 March 2014, have reflected the amount as shares transferred to MoR.~~

~~Thus, non-realisation of proceeds even more than two years after transferring the shares, indicated lack of effort on the part of the Government.~~

~~The matter was referred to Government in August 2015; reply had not been received (December 2015).~~

FINANCE DEPARTMENT

3.3 IT Audit of Computerisation of Salary Accounts

3.3.1 Introduction

With a view to assuring accuracy and timeliness in the generation of pay bills and related schedules required for producing salary bills of the establishments of Government Departments, an application software *viz*. Computerisation of Salary Accounts (COSA) developed by National Informatics Centre (NIC) was implemented by the Government of West Bengal during 2002-03. The system, with 16 modules (refer **Chart 3.1** at paragraph 3.3.7.1), runs in a standalone environment. It has SQL Server 2005 as back-end RDBMS and Visual Basic 6 as front-end tool.

3.3.2 Organisational set-up

The Finance Department controlled the application initially before its decentralisation in 2011. Finance Department entrusted the Drawing & Disbursement Officers (DDOs) with the responsibility of securing the access to COSA, taking regular back-up and training of man-power. As of March 2015, COSA is being used by more than 8000 DDOs across the State. The Finance Department, however, continues to issue instructions on the usage of COSA from time to time.

3.3.3 Audit Objectives

The objectives of IT Audit of COSA was to assess

- the extent to which COSA was being utilised for efficient management of salaries and entitlements;
- whether adequate controls were in place to ensure confidentiality, integrity and availability of data and
- whether measures were taken to ensure continuity of operations.

3.3.4 Audit criteria

The criteria for framing Audit comments were sourced from:

- West Bengal Service Rules (WBSR) and West Bengal Financial Rules (WBFR) and
- Generally accepted IT best practices.

3.3.5 Audit coverage, scope and methodology

The IT Audit of COSA was conducted between March and June 2015 covering the period 2009-15 through test-check of records/ data of 18 DDOs of seven Departments[9] (***Appendix 3.1***) in Kolkata and seven other districts. The districts were selected through stratified sampling based on geographical contiguity while the DDOs were selected through Simple Random Sampling without Replacement (SRSWOR).

Audit Findings

3.3.6 Limitations of the system

3.3.6.1 Multiplicity of administrative centres without proper training

The system being designed to work in a standalone environment, neither the Finance Department nor any other functional Department was in a position to utilise the data for any human resource, budgetary planning, etc. Moreover, multiplicity of administrative centres calls for higher degree of awareness and alertness among its users and administrators as compared to a web-based platform, which would have made the oversight on data management easier.

Besides, web-based platform would have facilitated easier integration of data with any future applications like Integrated Financial Management System (IFMS)[10].

However, IT Audit of various modules of COSA and their applications in various test-checked offices disclosed that not only the application was partially utilised owing to deficient training among the users, but there were instances of lack of control against possible misuse/ unauthorised use of the applications, as discussed in the succeeding paragraphs.

3.3.6.2 Lack of synchronisation with Treasury software

COSA Manual brought out by the Finance Department through NIC, envisaged integration of COSA database (containing salary details as well as personal details of the employees) into the Treasury software and IFMS. However, as per the present system in vogue, each DDO sends hardcopy of pay-bills generated through COSA application along-with two flat files (text file in .txt format) containing (i) all details of the pay-bills and (ii) all personal details of all employees for that particular month. Neither did the Treasury check the authenticity of the text file nor was the same being synchronised in the Treasury software. Treasury only checked the hard copy of the bills for any mistakes in calculation. However, incorrect information, if any, in the system-generated pay would remain undetected in absence of synchronisation between two different applications leaving scope for malpractice.

---

[9] *Backward Classes Welfare, Home, Labour, Land & Land Reforms, Health & Family Welfare, Higher Education and Information & Cultural Affairs*

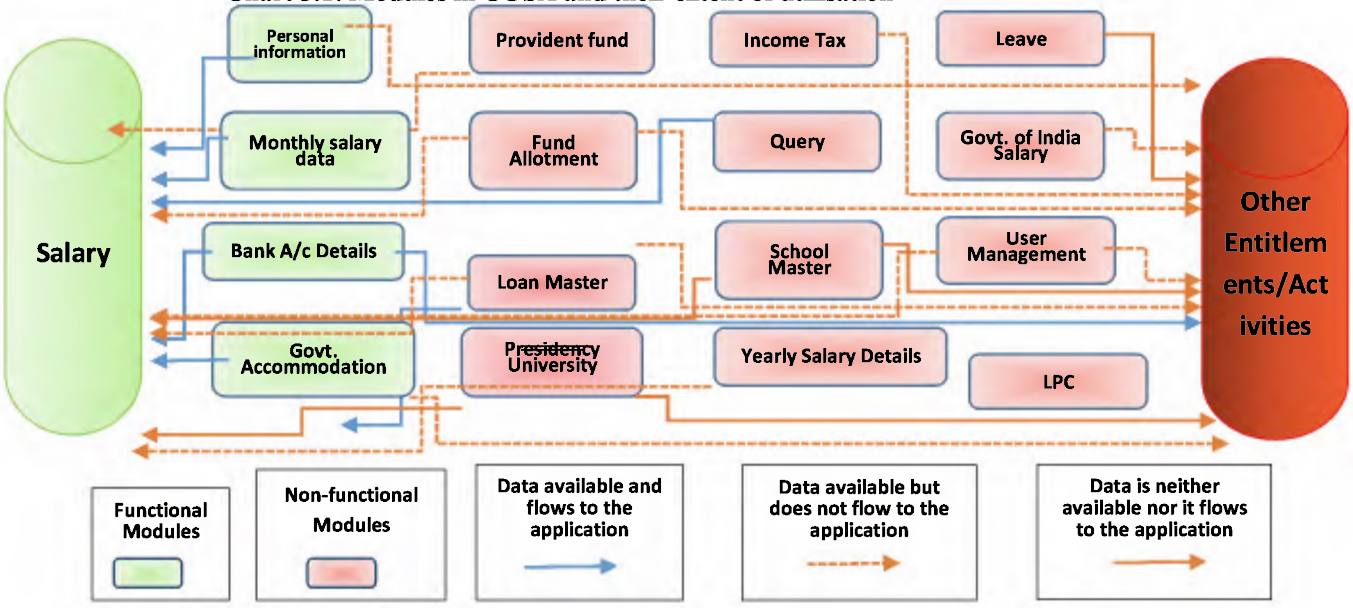
[10] *An e-enabled Integrated Financial Management System (IFMS) under implementation comprising all aspects of treasury and budget functions including integration of receipt and expenditure accounts of the State Government and its interface with Accountant General, Reserve Bank of India and Link Banks.*

3.3.7 Status of utilisation of the modules

3.3.7.1 Important modules directly relating to pay bills remaining unused

The application was designed with 16 modules. Apart from Pay Bill, the application included modules to capture various personal details of employees, Income Tax Module, Leave Details, etc. However, only four modules relating to pay bill were working in the test-checked units as indicated in **Chart 3.1** below:

Chart 3.1: Modules in COSA and their extent of utilisation



Thus, some modules containing information directly related to preparation of salary bills were not put to use in COSA. These included modules for Provident Fund, Loan Master, Income Tax, Leave and Funds Allotment. It was observed that in many of the test-checked offices, data relating to pay and allowances were manually fed into the system. This has undermined the very idea of automation behind introduction of COSA.

In three offices[11], usage of Last Pay Certificate (LPC) module had to be discontinued, after a brief period, due to faulty design of the module which barred the Administrator from editing the data once entered for any rectification, if necessary.

3.3.7.2 Insufficient training leading to non-use of modules

Test-checked DDOs attributed non-utilisation of all the modules to complexity of operating the modules for data entry and lack of training among the employees. The third party vendors were to arrange training programmes, immediately after installing the application in every DDO, for which they would be paid ₹ 5515 for each such programme. Finance Department instructed (March 2012) the DDOs to train at least two persons of the office of the DDOs, as well as of respective Treasuries for running COSA application package/preparing database/ updating database before generation of monthly salary bills. Sixteen out of 18 test-checked offices replied to audit that no such training programme was arranged. It was, however, observed that in 12 out of the 18 test-checked offices, the vendors were

[11] *Labour Commission, Bankura Sammilani Medical College & Hospital and Superintendent of Police, Jalpaiguri*

paid for training. As a result, the staff were not equipped to handle COSA efficiently.

3.3.7.3 Non-utilisation of COSA generated Employees database

As per the recommendation of the 13th Finance Commission, all State Governments were expected to build up a database of State Government Employees drawing salary from State exchequer. This also included the details of employees drawing salary by way of Grant-in-Aid and the pensioners. The 14th Finance Commission has also sought critical financial reports relating to salaries and pensions for its use from the State Government.

In order to meet up this requirement, Finance Department, Government of West Bengal, in its memo No. 305(65)/FY/P1E-180/2011 dated 06.02.2012 instructed all DDOs to prepare employees' database using COSA application. Accordingly, all DDOs were found sending two flat files generated through COSA application containing (i) all details of the pay-bills and (ii) all personal details of all employees as discussed in *para 3.3.6.2*. Moreover, in order to develop 'Employees Database', Finance Department instructed all Treasuries vide Memo No. 1829-F(Y) dated 01.03.2012 to capture all data generated by using COSA and sent by DDOs' end as input at the Treasury Computer Package from the first part and the other part of the data to be transmitted to 'Employees' Database Server' through Treasury Server linked with each salary bill of each DDO.

Scrutiny of records of the DDOs generated through COSA, as sent to treasuries revealed that the soft copies were never fed into the system by the Treasuries into 'Employees' Database Server'. Moreover, the quality of data relating to Human Resource as captured at the DDOs' end was very poor. The requirement of the 14th Finance Commission could not be met.

3.3.8 Security and adequacy of controls

IT Controls in a computer system represent policies and procedures that ensure the protection of the entity's assets and accuracy and reliability of its records. Finance Department had put (March 2012) the onus of securing the system by utilising users' access control mechanism on the DDOs. Audit, however, observed control deficiencies like absence of password policy, unrestricted allowance of super-user privileges (exclusive privilege to be enjoyed by the system administrator for editing entered data), inadequate access and validation controls, absence of antivirus, etc. as discussed in the succeeding paragraphs.

3.3.8.1 Password policy

A password policy is a set of Rules designed to enhance computer security by encouraging users to employ strong passwords and to change it periodically. A password policy is often part of an organisation's official regulations and should be strictly adhered to in order to safeguard the organisation's data. The following are the generally accepted best practices for a robust password policy:

- Passwords should be a combination of alpha-numeric-special characters;
- Failed log-in attempts are to be restricted by blocking the user-ID and

- Compulsory change of password after first log-in to change the password assigned by the Database Administrator and subsequent change of passwords at regular intervals.

No departmental directives on password: However, scrutiny revealed that no documented password policy was in place in any of the test-checked offices. Neither the Finance Department nor the individual Department had issued any instruction in this regard. There were no instructions for changing the default password and for changing passwords periodically. Consequently, all test-checked offices were using the default administrator user-ID and password since introduction of the application. This had undermined the security of the system.

3.3.8.2 Logical access controls

Logical access controls are tools and protocols used for identification, authentication, authorisation and accountability in computer information systems. It also restricts the user from accessing any part of the system, which is beyond his area of responsibility.

- ***All end users using administrator's user-ID and password:*** In the test-checked offices, the administrators (DDOs) did not create new user-IDs for end-users who would operate the COSA application in offices. Data analysis indicated that all end-users were using the administrator's user-ID and password, thereby enjoying full administrative privilege. This was also confirmed by 16 out of 18 test-checked offices (two offices did not furnish any reply). This left the application vulnerable to potential threat allowing end-users full access to the system.
- ***Absence of audit trail:*** Audit trail is a tool for the system administrator to obtain sufficient evidence in regard to the reliability and integrity of the application system. To achieve this, the audit trail should *inter alia* contain sufficient information to trace the history of activities in the system as well as sources of intentional and unintentional errors. The application does not have any provision for recording various aspects of audit trail like times of log-in and log-out by individual users, details of failed log-in attempts, user-wise access of modules, etc.

Use of identical user-ID and password by all users coupled with absence of any audit trail left the system vulnerable to unauthorised accesses and manipulation of data.

3.3.8.3 Validation Controls

The application was designed *inter alia* to capture vital information (like date of birth, date of joining service, PAN, etc.) of an employee, which had a bearing on his pay, service and statutory deductions. Hence, it was imperative that the system had in-built validation controls to ensure the quality of data entered therein. It was, however, observed that the system lacked such validation controls which affected the accuracy and validity of the captured data as illustrated below:

- ***Date of birth post-dating/ equalling date of joining the Government service:*** In 25 cases, employees' dates of birth were later than their dates of joining service, while in case of 4354 employees', dates of birth and their dates of joining service were the same.

- ***Wrong calculation of date of retirement:*** The mapping of date of retirement[12] was not properly done in the application resulting in several instances of wrong date of retirement. There were many cases where date of retirement was same as date of birth (1119 cases) or date of joining (14 cases), date of retirement pre-dating date of birth (117 cases) or date of joining (319 cases).
- ***Invalid or no PAN:*** In order to deduct TDS, it is mandatory for all Government employees to provide their Permanent Account Number (PAN) to the DDO. In case of 7587 employees, no PAN was available in the system. Further, considering that PAN is ten-character long with a defined alpha-numeric pattern, there should have been validation Rules embedded in the system. It was seen that there were no such validation controls and 337 cases were found by Audit where PAN numbers were in invalid format.
- ***No restriction on generation of bills after retirement of employees:*** The system was unable to automatically stop generation of pay bills after retirement of employees. It was seen that the data in respect of retired employees had to be manually deleted from the system to stop generation of pay bills beyond their dates of retirement. It was observed that pay bills were being generated in two test-checked offices[13] in respect of 118 employees, though they were supposed to retire as per system database. Kolkata Medical College and Hospital, while accepting the fact attributed this to wrong entry of data. The reply was not tenable as it represented failure in validation controls. Had there been such validation control in place, wrong/ junk entry of date of retirement would have been identified and rectified.

As all these data with erroneous information/ calculations were sent every month to the Treasury in flat files (as discussed in *para 3.3.6.2* earlier) along with the pay bills, the quality as well as authenticity of data remained highly questionable.

3.3.8.4 Absence of Antivirus Policy

Since the application deals with salary bills and captures personal details of all employees, it was desirable to maintain the computers free from any virus in any form so as to prevent any system fault and consequent data loss.

Absence of authorised antivirus in test-checked offices: Neither did any of the test-checked offices have antivirus policy nor was any authorised antivirus installed in the PCs, where the application was running. This was confirmed by all the 18 test-checked offices. Computers, earmarked for running of COSA, crashed in two[14] offices due to virus attack and the data could not be retrieved by the authority.

No restriction on use of external media: Further, there was no restriction as to handling of external media (pen drive, external drive, etc.) by the staff and the third party service providers exposing the system to virus attacks. This also posed

---

[12] *A Government employee retires from service on the last day of the month in which the employee attains the age of sixty, in case his date of birth falls on any day other than the first day of the month while in the latter case, the employee superannuates on the last date of the preceding month.*

[13] *Kolkata Police-19 and Kolkata Medical College and Hospital-99*

[14] *Offices of the Superintendent of Police, Jalpaiguri in December 2013 and District Welfare Officer, BCW, Purba Medinipur*

a security threat in terms of confidentiality of the personal information on employees.

3.3.9 Inefficient management control leading to embezzlement of Government money

Organisational and management controls represent the high level controls adopted by the competent authority to ensure that any application functions correctly, is fool proof and satisfies business objectives. There should be an IT Steering Committee for overall monitoring of the system.

While implementing COSA, Finance Department had not constituted any such Steering Committee nor was the same ever constituted by any of the Departments even after decentralisation of the application. None of the Departments visited, had directed its senior officials to periodically review the system at the grass root level. There was no system of cross verification of salary related information sent by a DDO vis-à-vis that maintained in the respective Treasury. Audit has come across an instance where the application was wilfully tampered to generate incorrect salary bill as discussed below.

Preparation of pay bills involves generation of pay bills as well as a summary of all pay bills known as outer sheet. Though the pay bills were non-editable and were printed directly from the application, the outer sheet was designed to be saved in an editable format.

In Sankrail BPHC, one Lower Division Clerk (LDC) was authorised with the administrative password to operate the application. This employee increased his pay and allowances by editing the outer sheet of bill generated from the system and syphoned out ₹ 1.50 crore between October 2012 and April 2015. This was detected in May 2015 and departmental proceeding started in June 2015.

Had there been a proper level of management controls in the system and had the system been properly designed to prevent saving any part of the pay bills in any editable format, such embezzlement could have been avoided.

3.3.10 Business Continuity Plan

Business Continuity and Disaster Recovery Plan aim to ensure that an organisation is able to accomplish its mission and it would not lose the capability to process, retrieve and protect information maintained in the event of an unforeseeable interruption or disaster leading to temporary or permanent loss of computer facilities. This calls for well-documented, tested and updated continuity and disaster recovery plans, regular back-up of systems software, financial applications and underlying data, etc. However, deficiencies were noticed in Audit in this matter as discussed in the following paragraphs.

3.3.10.1 Absence of Business Continuity and Disaster Recovery Plans

Neither the Finance Department nor the test-checked administrative Departments gave any instruction for preparation of business continuity and disaster recovery plans. Consequently, none of the test-checked offices had prepared such plans which compromised the capability to resume COSA operations in the event of physical interruption or logical upgradation.

3.3.10.2 Absence of data back-up

Regular data back-ups are an essential part of business continuity and disaster recovery plan. The system had an in-built facility for taking data back-ups. The Finance Department had given (March 2012) instructions to the DDOs to take back-up of updated database at the end of each day. The DDOs were, however, lax in taking regular data back-ups. In five out of eighteen test-checked offices, data back-up was taken in an interval of three months to fourteen months. Further, none of these 18 offices had kept data back-up outside the machine where the application was running. In two test-checked offices (Bankura Sammilani Medical College and Hospital and Jalpaiguri SP office), consequent to data loss, the entire data on employees had to be re-entered, as no data back-up was available.

3.3.11 Conclusion

Though one of the main objectives of timely generation of pay bills was achieved, the sub-optimal use of the modules coupled with questionable quality of data being fed left the system heavily dependent on manual interventions. Lack of training among the field level functionaries adversely affected meaningful implementation of the system, especially the application being standalone in nature without any centralised oversight/ control on data management. The system was exposed to risks of unauthorised manipulations of data as every user, in the absence of password policy, enjoyed unabated access to the database with all administrative privileges. Absence of audit trail in the system also made the accountability regime very weak. The data security was compromised by absence of an anti-virus policy, business continuity and disaster recovery plans and lack of seriousness of the DDOs in keeping regular data back-up.

The matter was referred to Government in July 2015; reply had not been received (December 2015).

~~FINANCE, PUBLIC HEALTH ENGINEERING, HEALTH & FAMILY WELFARE AND AGRICULTURE MARKETING DEPARTMENTS~~

~~*3.4 Payment of interest-free mobilisation advance to contractors*~~

~~In violation of the restriction imposed in West Bengal Financial Rules, Health & Family Welfare, Agriculture Marketing and Public Health Engineering Departments showed undue lenience to private contractors in allowing/ recovering mobilisation advances. No interest was realised by these Departments unlike Public Works Department.~~

~~As per West Bengal Financial Rules (Rule 227), advances should be paid to contractors, only in exceptional circumstances with the sanction of the Government, taking necessary precautions for securing Government against loss and for preventing the practice from becoming general rather than an exceptional one. The Public Works Department (PWD), which is a major Department involved in the execution of works under the Government of West Bengal (GoWB), has a system of allowing mobilisation advances for big works and~~