Chapter V
General Sector

CHAPTER V
GENERAL SECTOR

5.1 Introduction

The audit observations relating to various State Government departments and their units under General Sector are featured in this chapter. During 2017-18, against a total budget provision of ₹ 3,515.62 crore, a total expenditure of ₹ 3,188.88 crore was incurred by 15 Departments under the General Sector. The Department-wise details of budget provision and expenditure incurred there-against are shown in the following table.

Table No. 5.1.1 Budget provision and expenditure of Departments in General Sector during 2017-18

(₹in crore)

Sl. No.	Department	Budget Provision	Expenditure
1	Planning	426.93	162.33
2	Election	28.46	12.86
3	Police	1,420.14	1,299.56
4	Finance *	1,277.15	1,416.84
5	Local Fund Audit		
6	Stationery and Printing	5.77	5.45
7	Administration of Justice	117.08	65.35
8	Land Revenue, Stamp and Registration and District Administration	110.57	110.57
9	Fire Protection and Control	13.85	10.09
10	Secretariat	85.87	80.29
11	Vigilance	3.93	3.64
12	Manipur Public Service Commission	5.68	5.24
13	State Academy of Training	6.52	4.62
14	Governor Secretariat	5.02	5.01
15	Rehabilitation	8.65	7.03
Total		**3,515.62**	**3,188.88**

Source: Appropriation Accounts.

** Excluding Appropriation No. 2 – Interest Payment and Debt Services.*

Apart from budget allocation by the State Government for various departments, the Central Government has been transferring a sizeable amount of funds directly to the implementing agencies of the State Government for implementation of various programmes of the Central Government. During 2017-18, out of total amount of ₹ 54.67 crore released directly to the different implementing agencies, no funds were released under General Sector.

5.1.1 Planning and execution of audit

Audit is conducted in accordance with the annual audit plan. The audit units are selected on the basis of risk assessment carried out keeping in view the topicality, financial significance, social relevance, internal control system of the units, and occurrence of defalcation/ misappropriation/ embezzlement as well as past audit findings *etc*.

Inspection Reports are issued to the heads of units as well as heads of departments after completion of audit of a unit. Based on the replies received, audit observations are either closed or departments / units are advised to take further remedial measures as required. Important audit findings are processed for inclusion in the Audit Report of Comptroller and Auditor General (CAG) of India for placing of the same before the Legislative Assembly.

Audits were conducted during 2017-18 involving an expenditure of ₹ 3,316.71 crore including expenditure of previous years of the State Government under General Sector, as shown in ***Appendix 5.1***.

This chapter contains one Information Technology Audit *viz.*, "Information Technology Audit of Computerisation of Personnel Information System" and one compliance audit paragraph as discussed in the succeeding paragraphs.

INFORMATION TECHNOLOGY AUDIT

FINANCE DEPARTMENT

5.2 Information Technology Audit of Computerisation of Personnel Information System

The Computerisation of Personnel Information System (CPIS) formerly known as Manipur Government Employees List (MGEL) is an Information Technology application of the Government of Manipur to maintain the database of employees of the Government of Manipur. CPIS is a flagship e-governance application of the Government of Manipur.

CPIS seeks to assist administration by carving out a structured database of all the Government employees, offices and departments by capturing employees profile[154], allotment of unique Employee Identification Number (EIN), name, date of birth, date of entry into Government service and Human Resources details like sanctioned posts and persons-in-position.

The audit of CPIS was carried out during April 2018 to August 2018 with a view to see whether the CPIS application was functioning efficiently and effectively and achieved intended objectives. The main audit observations are highlighted below.

Highlights

- *CPIS data was found to be factually incorrect and incomplete. Most of the incorrect and incomplete data was imported from the legacy system i.e., Manipur Government Employees List without any further validation and checks. Application Controls in the system were weak as it allowed entry of non-relevant data.*

(Paragraphs 5.2.7.6, 5.2.8.1, 5.2.8.2 and 5.2.9.2)

- *Inordinate and frequent delays were noticed in the departments in preparing and sending input Forms to the Directorate of Management Information System (DMIS) for updating CPIS.*

(Paragraphs 5.2.8.3)

- *Directorate of Management Information System had not prepared any formal IT policies to establish the control and security culture in the organization. These included absence of policies on IT Security, Access, Users' Passwords, Business Continuity, staff development, etc.*

(Paragraphs 5.2.9.1)

- *Directorate of Management Information System had not carried out any formal risk assessment exercise to identify possible risks to CPIS and IT assets with a view to devising suitable controls to manage these risks to an acceptable level.*

{Paragraphs 5.2.9.1 (a)}

[154] Employee name, father name, date of birth, date of joining service, appointment order, name of office *etc*.

- *Senior management had not been very active in the implementation of CPIS as neither were any formal policies formulated nor the system was monitored effectively by them.*

(Paragraphs 5.2.10)

- *The Departments did not use CPIS for deciding staff deployment and transfers effectively. On the one hand, many offices were found with no manpower while on the other hand, many offices had manpower in excess of their sanctioned strength.*

{Paragraphs 5.2.8.4 and 5.2.9.2 (b)}

5.2.1 Introduction

5.2.1.1 Background: MGEL, CPIS and CMIS

In pursuance of the recommendation of the XIth Finance Commission and also on the instructions of the Ministry of Finance, Government of India for preparation of budget, an attempt was made to compile a list of the entire Government employees wherein all employees were allotted a unique code number for their identification.

In 2002-03, the Finance Department, Government of Manipur entrusted the above work to the National Informatics Centre (NIC) Manipur. The Manipur Government Employees List (MGEL) software was developed using MS Access and data entry of the employee profile by the respective departments was completed in 2003. In September 2005, the Finance Department, Government of Manipur had taken a decision to verify the data captured in the database by the end of March 2006 which was completed by the mid-October 2006.

In terms of Rule 6 of the Fiscal Responsibility and Budget Management Rules, 2006, preparation of a list of the Government employees became a mandatory requirement for presentation of the annual budget. Moreover, for deployment of suitable and adequate staff to improve the delivery of public services to the hilly and remote areas, the Government wanted to integrate profiles of the institutions/offices[155] of the departments into the existing MGEL database.

Thus, the new database integrating MGEL data with the profiles of the institutions/offices of the departments resulted in creation of the Computerisation of Personnel Information System (CPIS) in 2006. The responsibility for functioning of CPIS has been entrusted to the Directorate of Management Information System (DMIS), Finance Department, Government of Manipur with effect from January 2010.

Further, the Finance Department, Government of Manipur in collaboration with NIC, Manipur had planned to roll out, by March 2014, a new web-based application system called Central Management Information System (CMIS) to replace the existing CPIS. However, rolling out of CMIS was still under process. The operation was required to be done at the level of Drawing Disbursing Officer (DDO), Head of Department, Administrative Department

[155] Sanctioned post, post creation order and date of creation of post.

and Finance Department (Directorate of MIS). In addition to the modules available in CPIS, a dynamic pay roll module would be available in CMIS. Presently, the system is being implemented by 40 out of 957 DDOs on Pilot basis (December 2018).

5.2.1.2 CPIS organisational structure

CPIS functions under the overall guidance of the Chief Secretary and under the operational control of the Directorate of Management Information System (DMIS), Finance Department, Government of Manipur. The Nodal Officers are appointed in each Department to ensure that information pertaining to CPIS is timely prepared and sent to DMIS in the prescribed formats by the departments under their signature and seal. Information processed through CPIS application is certified for their correctness and accuracy by DMIS, Finance Department.

5.2.1.3 Objectives of CPIS

The objectives of the CPIS were to:

- Provide accurate details of the staffing pattern of the employees including the sanctioned posts and person-in-position in each Government Department;
- Capture detailed information of each employee appointed against a sanctioned post;
- Update employee data on promotions, transfers, retirements, *etc.*;
- Facilitate policy decision on deployment, redeployment and transfer of employees;
- Improve delivery of public services in hilly and rural areas; and
- Estimate budget for salaries, grants of DA, *etc.*

5.2.1.4 CPIS System Architecture

CPIS application has been developed in a Client-Server architecture using .NET and SQL Server as database with the following system requirements:

- **Server:** - The server has Windows Server 2003 onwards as operating system (OS), SQL Server 2008 R2 as RDBMs, Microsoft.NET 4.0 as framework and IIS as web server respectively.
- **Client (Desktop application):** - This has Windows XP and above as OS and Microsoft.NET 1.0 as framework respectively.
- **Client (Report Module):** This has Linux / Windows as OS and IE, Mozilla Fire Fox as browser respectively. This is a web-based Reporting module.

Client Application**:** This application is used for data entry and updating. The different modules available under this application are enrolment for new recruits, transfers and postings, promotions, termination, sanctioned post updating, *etc*. Information is accepted from the line departments in 13 prescribed forms. It has five levels of users with different privileges granted for security measures. They are Super User, Administrator, Data Manager and Operators 1 and 2.

Reporting Module: The database updated by the application software is published on the CPIS web portal *(http://cpis.man.nic.in)* to provide various information in the form of reports for different category of users.

Public Domain Reports: This can be used to view employee profile, department-wise and office-wise employees details and also the list of employees rejected by CPIS.

Secured Domain Reports: Users are required to login using their own user IDs and passwords. Once logged in, the users are allowed to view the following reports based on the permission granted to them:

- Nodal Officers of line departments can view details of their own departments like category-wise sanctioned posts, employee details, vacancies, *etc*.
- DMIS can browse the report for all departments as they are the certifying authority of CPIS reports which are used for drawal of monthly salary.
- Treasury Officers can view details of all departments and they are to check and compare CPIS list of offices concerned downloaded from CPIS website with the list of employees sent by DDOs for drawal of salary.
- Top Management: Information available under this category is meant for monitoring and administration purposes. Hence, only macro level reports are generated.

5.2.1.5 CPIS Workflow

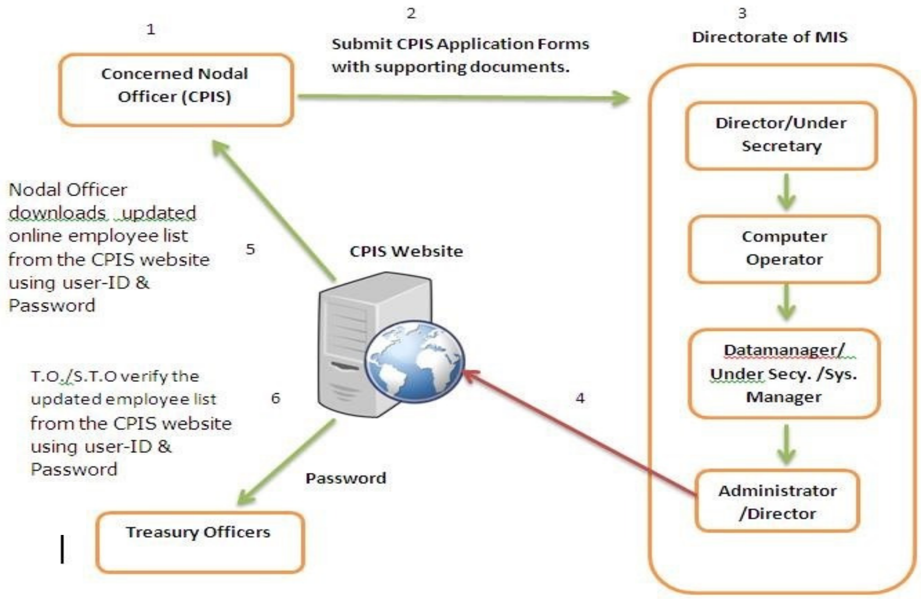
The Nodal officer (CPIS) of the Department sends proposals in prescribed Forms along with the relevant documents to DMIS for any change in CPIS database as a result of change in employee list, sanctioned posts, staff transfers, promotions, corrections, terminations, *etc*. The Nodal Officer also downloads data for his department and supplies the same to the DDOs concerned.

DMIS on receipt of the forms from the Nodal Officers checks the forms and enclosed documents for accuracy and completeness and if satisfied, updates database. Data entered by the Computer Operators are verified by the Data Managers (Under Secretary / System Manager) and then ultimately uploaded to the database by the Application Administrator (Director of the MIS). The incomplete/incorrect forms are returned by DMIS to the Nodal Officers concerned by stating reasons for their rejections.

Treasury Officers check and compare CPIS list downloaded from CPIS website and compares the same with the list of employees sent by DDOs for drawal of salary.

Manipur Public Servants' Personal Liability Act (MPSPL) 2006, which provides for fixing of responsibility on Public Servants and makes them personally liable for irregular action, is enforced in order to ensure that Nodal Officers do not manipulate or provide vague data. The CPIS workflow is depicted in the following chart.

Chart No. 5.2.1 CPIS workflow


1
Concerned Nodal Officer (CPIS)
2
Submit CPIS Application Forms with supporting documents.
3
Directorate of MIS
Director/Under Secretary
Computer Operator
Datamanager/ Under Secy. /Sys. Manager
Administrator /Director
4
CPIS Website
5
Nodal Officer downloads updated online employee list from the CPIS website using user-ID & Password
6
T.O./S.T.O verify the updated employee list from the CPIS website using user-ID & Password
Password
Treasury Officers

Source: Directorate of Management Information System.

5.2.2 Scope of audit and sample selection

The scope of audit included the following:

a. Examination of CPIS system;

b. Examination of controls in CPIS applications;

c. Analysis of CPIS Database[156]; and

d. Ascertaining system effectiveness.

The audit methodology contained test check of the implementation of CPIS in 15 selected Nodal Officers (out of 60 Nodal Officers) of Departments covering four treasuries (two valleys and two hills) out of 11 treasuries for the period 2013-14 to 2017-18 was carried out. During the audit process, records of 57 DDOs (of selected Nodal Officers) were examined in detail. The sampling was done using the method of Stratified Random Sampling using IDEA software.

5.2.3 Audit objectives

The objectives of the IT audit were to ascertain whether:

- The planning and development of the CPIS application was proper and in line with the requirement of the Government;
- The system was functioning efficiently and effectively to achieve the intended objectives of Government;
- The security and controls associated with CPIS were adequate; and
- Adequate and effective mechanism existed for monitoring and evaluation of the CPIS application.

[156] As on 19 August 2018.

5.2.4 Audit criteria

Audit findings were benchmarked against the following criteria:

- Government rules, regulations and policy on recruitment, transfer, promotion, staffing pattern *etc*.
- Notifications issued by the Government from time to time**.**
- Internationally accepted best IT practices.

5.2.5 Audit methodology

The audit methodology included holding an Entry Conference (April 2018) in the beginning of audit with the Director (MIS) and his officers and officials of National Informatics Office, Manipur, interviews with CPIS personnel/ stakeholders, issue of questionnaires, control assessment, physical verification, test check of records and data analysis. CPIS data was analysed using Computer Assisted Audit Techniques (CAATs) and some of the findings were cross checked for further verification. The draft Audit Report was forwarded to the Government of Manipur on 08 November 2018 for seeking their comments. The Department vide their letter dated 19 November 2018 sent their comments. The Exit Conference was held on 19 November 2018 with the Special Secretary (Finance) and Director (MIS) and his officers. The replies of the Government have been incorporated in the report at appropriate places.

5.2.6 Acknowledgement

Indian Audit and Accounts Department (IA&AD) acknowledges the cooperation and assistance extended by the State Government and respective offices in providing necessary information and records during the course of audit.

Audit Findings

The important issues/points noticed during the course of audit are given in the succeeding paragraphs.

5.2.7 Planning and Development

5.2.7.1 Feasibility Study not conducted

For successful implementation of any project/scheme, a feasibility study is required to be undertaken to ascertain the viability of the proposed project/scheme.

Audit scrutiny of records revealed that the Department had not conducted any feasibility study to ascertain the physical and technical viability of CPIS. Without conducting such a feasibility study, the NIC was engaged to develop the CPIS application which was not in consonance with the complete requirements of the Department as explained in the subsequent paragraphs.

5.2.7.2 Non-existence of User and System Requirement Specifications

To ensure that the application proposed to be developed meets organizational objectives, detailed functional requirements of the users popularly known as User Requirement Specifications (URS) are required to be collected as part of the planning for the development of an application. URS becomes the main focus and basis for the design and development of the application, thereby, ensuring the usefulness and effectiveness of the proposed system.

Similarly, an assessment about the hardware and technical specifications required for the development and smooth operation of the system, *i.e.,* System Requirement Specifications (SRS), is required to be prepared.

Audit scrutiny of records revealed that detailed URS was not prepared and provided by the Finance Department to the NIC at the initiation of CPIS. Hence, the application was designed and developed by NIC without any URS, thus, limiting the usefulness of the application. Absence of URS also impacted management's ability due to which it failed to capture full employee details, weak logical access control and application controls, *etc*., as discussed in the succeeding paragraphs **{Paragraph Nos. 5.2.7.4, 5.2.9.1(g) and 5.2.9.2}**. Absence of documented URS would also handicap any efforts to be made in future by the organization or by Audit to evaluate the effectiveness and usefulness of CPIS in meeting the intended objectives. Similarly, SRS was not prepared before deciding to develop CPIS.

5.2.7.3 Non-existence of User Manuals

User Manual is a document which describes essentially all of the software's functionalities for an application user. The User Manual provides important information on 'how to use a software' to the end-users. User manuals help in the smooth operation of the application in addition to being a useful input for the staff training and development.

During the course of audit, it was noticed that User Manual for Directorate of Management Information System (DMIS) staff only was prepared. However, User Manual for treasuries and departments which forms the major chunk of the users was not prepared. User Manuals help, guide and form a reference book for all the newly appointed Nodal Officers, Treasury officers and DDOs who were yet to attend any training provided by the NIC/DMIS. Detailed guidelines for the implementation of the project like qualifications, duties and responsibilities of the Nodal officers, timeframe for the submission of various forms to DMIS for CPIS updating, penalty for non-adherence, timeframe for the verification and certification of data by the Finance Department were not prepared to provide necessary directions as part of the CPIS planning and development. This resulted in delay in submission of forms to the DMIS on account of transfer, promotion, retirement, *etc*., making the CPIS data unreliable.

On being pointed out by Audit, the Department replied that User Manual was not prepared as the Departments and Treasuries were given 'hands-on' training at the initial stages of CPIS and their role was limited to sending of proposal through hard copies. The reply of the Department was not tenable as User Manuals are useful for ensuing smooth working of CPIS. Moreover, User

Manuals are also required for use as a reference book for the purpose of providing training to the staff members concerned as also to Nodal Officers, Treasury officers and DDOs.

5.2.7.4 Non-provision for capturing of full employee details

In the absence of URS, the CPIS application could not be designed and developed to meet all the functional requirements of the proposed system. CPIS was not having provisions (fields/data columns) to capture basic HR/employee information like employee address (permanent and temporary), GPF Account number, PAN number, Permanent Retirement Account number (PRAN), *etc*. The entire name is captured in one column and not in the desired format *i.e.*, separate columns for First name, middle name and last name. In the cases of 39,252 (50 *per cent*) out of 78,195 employees, names were incomplete and showing initials only in the system.

Further, the application was made 'live' before its testing to ascertain whether it was meeting all necessary functional requirements. Resultantly, the missing gaps could not be flagged and incorporated in the application.

Moreover, in the absence of URS and SRS, Audit was unable to fully assess as to what extent the intended benefits of the CPIS had been achieved.

5.2.7.5 Non-provision of separate columns for Pay Scale, Grade Pay and Pay in Pay Band

On the recommendations of the 6th Pay Commission and as per Manipur Services (Revised Pay) Rules, 2010, pay of an employee is described in the form of Pay Scale, pay in Pay Band, Grade Pay and Basic Pay (Pay-in-Pay Band *plus* Grade Pay). Annual increment will affect the pay in Pay Band and Grade Pay will be affected in the case of grant of any financial upgrading due to Promotion, Assured Career Progression (ACP)/ Modified Assured Career Progression (MACP), *etc*.

Examination of CPIS database and online certified employee list generated by the departments revealed that there was no separate column to capture the Grade Pay as the same was found clubbed with the Pay Scale. The absence of separate column for Grade Pay would make it difficult to generate Grade-wise information required for financial and budgetary planning. Such missing data in CPIS would also make it impossible to use CPIS for generation of monthly salary, thus, significantly limiting the utility of the system.

On this being pointed out by Audit, the Department accepted audit observations and stated that CPIS indicates Pay-Scale and Grade Pay clubbed together because at the time of development of application, the Grade Pay component was not existing. However, for pay details, a new payroll module had since been incorporated in CMIS (to be rolled out shortly) which will indicate all details of Pay. The reply of the Department was not acceptable because the pay as per 6th Pay Commission pay scales was being drawn and paid to the State Government employees since 2010, and hence, the requirement should have been incorporated long ago in CPIS, but it was not done.

5.2.7.6 Non-validation of MGEL data before importing to CPIS

Data in the earlier Manipur Government Employee List (MGEL) application, created in 2002, was imported to CPIS in 2006 and additional information like the sanctioned posts, office name, department names, *etc*., were incorporated in the application. However, the accuracy and completeness of MGEL data was not verified before importing it to CPIS. Though CPIS data was reportedly verified by the Finance Department, numerous errors were noticed by Audit even in the basic details of employees *viz.,* name, date of birth, date of joining, title, gender, *etc*. This indicated that the MGEL data was not properly verified and corrected neither by the Finance Department nor by the user department as would be evident from the succeeding paragraphs.

It was observed during audit that out of data relating to 78,195 employees, the word "correction" was written under remarks column in the case of 6,332 employees (*eight per cent of the total database*). This indicated the degree of errors in the imported MGEL data. It was also observed that the correction process was further complicated by DMIS by issuing an order (April, 2018) which required a speaking order from the Administrative Department for every correction in the employee's data.

Thus, the MGEL data was not verified and corrected by the Departments concerned or Finance Department before importing the same to CPIS, thereby allowing the errors/missing gaps existing in MGEL to continue in CPIS. The continuation of missing/incorrect employee details in CPIS invariably undermines the usefulness and effectiveness of the system.

The Department agreed with audit observations stating that MGEL data imported to CPIS had errors and that 6332 employees' details were already corrected as indicated in this report.

Recommendation (20): DMIS and the Nodal Officers should take urgent measures to verify, update and correct CPIS data wherever found necessary to make it useful, relevant and reliable.

5.2.8 Efficient and effective functioning of the system

5.2.8.1 Inaccurate details of staffing pattern

(a) Presence of data related to the retired employees in database

The age of superannuation for employees of the Government of Manipur is 60 years *w.e.f.* 29 November 2010 and 65 years for teaching staff of State Government colleges *w.e.f.* 28 February 2013. Timely removal of the data relating to the retired employees from CPIS was inevitable in order to provide accurate details of the staffing pattern, rationalize transfer and posting, prepare realistic budget and to assess vacancy position and new recruitments, *etc*.

It was, however, observed during audit that the data relating to 5,808 employees who had crossed the retirement age, was still existing in the CPIS database. This was due to the fact that the DMIS updates the data relating to retired employees in CPIS database only when CPIS forms along with related documents are submitted by the Departments concerned. However, the Departments usually delay the submission of necessary forms to the DMIS for updating employee details in CPIS. Further test-check of 29 such employees in 10 sampled offices revealed that they were not actually drawing salary after the date of their retirement but forming part of database of CPIS. The number of years since these retired employees were part of the database after their date of retirement is as detailed below.

Table No. 5.2.1 Summary of employees whose details have been kept in CPIS database in spite of their retirement

Sl. No.	Number of years after retirement	Number of employees
1	Less than 1 year	1,954
2	Between 1 to 5 years	3,465
3	Above 5 years	389
Total		**5,808**

Source: Data from CPIS database.

Thus, the number of employees in the CPIS database was not *prima facie* accurate defeating the objectives of CPIS to provide accurate details of staffing pattern against sanctioned posts and to update information in respect of retired employees in order to facilitate taking policy decision on deployment, re-deployment and transfer of employees, bringing out vacancy position and preparation of a realistic budget for their pay and allowances.

(b) Non-removal of temporary staff from CPIS on their discontinuation

Employees whose services are discontinued by the Government should be immediately removed from the active CPIS database. This would help Treasury Officers and DDOs to stop drawal of their salary *etc*. However, test check of records of Revenue Department revealed that 28 temporary posts of the Department were not extended by its Administrative Department vide W/T No. 1/31/89-R (Pt-III) dated 11 July 2011 and the department instructed not to release pay and allowances to them *w.e.f.* 01 March 2011.

It was, however, found that out of 28 such posts, the details of 17 persons were still available in CPIS database as active working employees. Audit cross checked the audit findings with respect to the two sampled offices *viz.,* Deputy Commissioner (DC), Imphal West and DC, Chandel and found that the pay and allowances were stopped in the case of all the four employees *w.e.f.* 01 March 2011 in pursuance of the order *ibid*.

The Department replied that the data relating to temporary employees were not removed as the Revenue Department had not sent proposals for removal of the data of persons concerned. However, reflection of the discontinued employees in CPIS resulted in inaccurate details of staffing pattern and wrong information of persons-in-position of the offices which had adverse impact on the integrity, effectiveness, reliability and usefulness of the system.

(c) Utilization of employees at places other than actual place of posting

One of the main objectives of CPIS was to rationalize transfer and posting of the employees and to deploy employees in accordance to the sanctioned posts and to guard against the deployment of employees at places other than actual place of posting, which was in violation of Government Rules and irregular.

The Finance Department had prohibited such cases of deployment and declared the same as irregular within the meaning of Manipur Public Service Liability Act, 2005.

Scrutiny of records of the sampled offices revealed that the services of 104 employees shown as posted in 36 offices were being utilized in other offices of the department where they were not actually posted. Further, 15 Veterinary Field Assistants (VFA) and Veterinary Attendants (VA) were found deployed in the Governor's Secretariat under the Department of Personnel and Administrative Reform where there was no sanctioned post of VFA and VA.

Thus, these employees were drawing their salary from the office where they were shown as posted while they were actually working in some other offices. This defeated the very objective of CPIS to provide accurate staffing pattern for rationalization, transfer and posting of employees. Moreover, they were not performing jobs for which they were actually appointed.

On the above being pointed out by Audit, the Department accepted audit findings on deployment of employees at places other than their original place of posting. The Department, however, stated that prevention of such irregular deployment was not in the purview of CPIS. The reply was not acceptable as one of the objectives of CPIS was to prevent deployment of employees at places other than at the places of their actual posting.

5.2.8.2 Non-capturing of detailed information of each employee

One of the main objectives of CPIS was to capture detailed and correct information of employees appointed against sanctioned posts. However, on scrutiny of CPIS database and examination of records of the sampled departments, the following deficiencies were observed:

(a) Non-updating of Pay Scale and Basic Pay

The details relating to Pay Scale, Grade Pay and Basic Pay of employees should be accurate in the CPIS database for ensuring preparation of a realistic budget and to ensure the correct payment of salary. The State Government employees started receiving salary *etc.* as per 6th Pay Commission Recommendations *w.e.f.* 1 January 2010. However, the pay scales, grade pay and basic pay of 45,134 out of 78,195 (57.7 *per cent*) employees were not updated even after a lapse of eight years of the implementation of the said recommendations. These non-updated pay scales shown in the CPIS pertained to 4th and 5th Pay Commission scales of pay. Audit observed that the details of salary were updated in CPIS only when the forms for promotion, transfer, correction, *etc.*, were submitted by the respective departments.

Audit also found that the correction forms submitted by the Agriculture Department[157] for updating of pay scale and basic pay of their employees were not updated by the DMIS. As a result, the Treasury Officers and DDOs could not use CPIS data for preparation of salary as CPIS was not able to provide accurate and complete information. As such, the Treasury and DDOs were

[157] During May to June 2014. Out of correction forms submitted for 28 DDOs, only 5 DDOs corrections were updated by DMIS.

using CPIS only to ascertain the names of employees in CPIS, and once ascertained; the salaries prepared locally by the DDOs were being verified by the Treasuries.

The Department stated in reply that the pay details were made available to the Nodal Officers through CPIS web for updating CPIS data. Reply was not acceptable as the CPIS data was not being updated regularly. Thus, the incidences indicated above could have been avoided had the data been updated regularly to ensure optimum utilisation of CPIS.

(b) Non-capturing of office order number and date

Joining of any new recruit, transfer, promotion or termination is effected only after issue of an office order by the competent authority. For CPIS updating, the Nodal Officers are required to mention the office order number and date in relevant forms and to enclose the relevant office orders without which the updating will not be effected.

The data entry operators were required to check and enter the office order number in the updating process. The data entered are to be verified and certified at two different levels by the Data Manager and the Administrator respectively.

Audit observed that CPIS has the fields to capture the data relating to employees' name, title, gender, office name, office order number, order date, *etc*. However, the analysis of CPIS database revealed that neither the office order numbers nor the order dates were found captured in 931 cases out of total 78,195 employees whereas in 48 cases, the office order dates only were found. These reflected deficiencies in data entry as well as data entry verification in CPIS. Non-availability of the source orders relating to the recruitment, transfer, promotion or termination of the employees in CPIS affects the integrity and usefulness of data. Absence or ineffectiveness of verification and supervision process in CPIS does not ensure accuracy and completeness of data updating. Thus, to this extent the information captured in CPIS was incomplete in these cases. This affects both the integrity of data as well as utility of the CPIS.

5.2.8.3 Delay in updating of data on recruitment, promotion, transfer, *etc.*

Updating of CPIS data is a continuous exercise and prompt update of any changes in the employee details is required for timely and correct payment of salary in addition to achieving other objectives of CPIS. Though, no timeframe has been fixed by the Government for submission of forms, Finance Department had requested (June 2013) all the departments to arrange for timely submission of forms to DMIS so that the salaries of employees are not unnecessarily withheld.

Audit found that there was no mechanism devised to monitor and prevent delays in updating of employee details in CPIS. Inordinate delays in preparing and sending input Forms by the Nodal Officers to DMIS were noticed. In some cases, DMIS also did not promptly key in the Forms received from the departments. Though the Finance Department had issued instructions for submission of necessary forms, the delays in updating of employee details in CPIS were noticed by Audit as explained below:

- **Direct recruits**: In the case of 53 out of 55 employees of four[158] selected Departments, delays in issue of Employee Identification Number (EIN) ranging from one to 44 months were observed.

- **Delay in updating on promotion**: In case of 71 out of 72 test checked employees of four[159] selected Departments, employees' data on account of promotion was not updated in a timely manner. The period of delay ranged from one month to eight years.

- **Retired/ Superannuated employee**: Due to the inaccuracy in the date of birth captured in CPIS, the details of retired employees were not removed by DMIS. Rather, they waited for the submission of forms by the Nodal Officers concerned. Consequently, data of many retired employees were present in the database. The Department also did not submit the forms in a timely manner for termination and the delays ranging from one month to five years were noticed in updating termination forms in case of all 239 test-checked employees who belonged to 12[160] selected Departments.

- **Organized services**: Employees of Organized services having an EIN were exempted from the purview of CPIS since September, 2009 allowing them to draw salaries even if their details were not updated in CPIS on account of transfer, promotion, *etc*. The Finance Department vide OM dated 25 September 2009, had asked Department of Personnel & Administrative Reforms, Government of Manipur to update CPIS through DMIS within one week from the date of issue of order. Despite Finance Department's order *ibid*, CPIS data had not been updated and the Organized services officers had been able to draw their salary without updating CPIS. It was observed in the nine selected DDOs that out of 49 officers of Organized services present in the employee list (September, 2018), the details of 28 officers were not updated. Further, the details of 17 officers posted and working in the selected offices were not reflected in CPIS. Test check of the forms of selected Departments in DMIS further revealed that updating of data of the officers of Organized Services was delayed up to five years.

- **Transfer and posting**: The Government of Manipur vide Order No. 1 June 2005- FB dated 6 April 2006 and 8 August 2007 provided for updating of CPIS in connection with transfers and postings. Input forms for such changes are required to be submitted in the appropriate forms as soon as possible so that salaries could be drawn on time. However, in 24 out of 25 test checked cases of transfer/posting of employees belonging to six[161] selected Departments, Audit found delays in updating of data ranging from one month to 18 months.

[158] Agriculture, Assembly Secretariat, Forest and Revenue Departments.

[159] Agriculture, Veterinary & Animal Husbandry, Forest and Home Departments.

[160] Forest, Commerce & Industries, Home, Command Area Development Authority, State Academy of Training, Public Works Department, Agriculture, Education (S), Education (U), Veterinary & Animal Husbandry, Assembly Secretariat and Revenue Departments.

[161] Forest, Agriculture, Command Area Development Authority, State Academy of Training, Public Works Department and Veterinary & Animal Husbandry Department.

Thus, due to the inaction/delays both by the Department and DMIS in updating the CPIS in a timely manner, the CPIS database was inaccurate and incomplete affecting the reliability, integrity and effectiveness of the CPIS.

While agreeing with audit findings, the Department stated that the delay in updating data on recruitment, promotion and transfer *etc*., was due to delay in submission of proposals for updating from the Departments concerned. However, under the new CMIS, the updating of database would be on online basis in which there would not be any delays.

Recommendation (21): Necessary mechanism should be devised and strictly enforced to ensure that Input Forms are promptly prepared and sent to DMIS for updating the CPIS. Forms could be filled in online, expediting the whole process.

5.2.8.4 Non-utilization of CPIS data on deployment, re-deployment and transfer and posting of employees

One of the major objectives of CPIS was to help Government in policy decision on deployment, re-deployment and transfer of employees by the Departments and also to improve delivery of public services all over the State, both in the hilly and rural areas.

Examination of records of transfer and posting files of three selected Departments *viz*., Veterinary and Animal Husbandry, Medical and Health Services and Public Works Department (PWD) revealed that transfers and postings were done in a piecemeal manner on personal requests of the employees or on the recommendations of the Member of Legislative Assembly (MLAs) or other influential individuals or officials.

Further, the analysis of CPIS data in three Departments revealed that there was disproportionate distribution of employees in various offices of Departments. Out of 2889 offices, no employee was posted in 101 offices though they had sanctioned posts whereas there were 1,185 offices where persons-in-position was full as compared with sanctioned strength. The details are shown in the following table.

Table No. 5.2.2 Disproportionate distribution of employees in the Departments

(In numbers)

Sl. No.	Name of Department	No. of Offices	No. of offices with zero Persons-in-Position	No. of offices with full Persons-in-position
1	Education (S)	2,201	57	915
2	Medical & Health Services	641	36	270
3	PWD	47	8	0
Total		**2,889**	**101**	**1,185**

Source: CPIS data.

Audit further observed that the requisite staff was not posted in one selected office *i.e.*, ANM Training Centre, Churachandpur during the last five years. The Training Centre had one post of Principal, three posts of Public Health Nurses (PHNs) and four posts of Sister Tutors. However, only one Principal and two PHNs were posted since 2012. Two PHNs had also retired in February

2014 and April 2016 respectively. The posting of tutors was not done at the training centre despite several requests made by the Principal.

Further, it was also observed that CPIS forms for transfers submitted by the Departments were rejected by DMIS as there was no vacant post in the offices in which they were transferred.

On this being pointed out, the Department replied that the transfers and postings of employees and their deployment were being fully controlled by the Administrative Department concerned.

Thus, though the CPIS application had embedded controls to reject the number of manpower posted exceeding the sanctioned posts, CPIS was not being used in making transfers and postings in the Departments, defeating the intended objective of the System.

Recommendation (22): The Departments should make use of CPIS/CMIS in deployment of staff in offices depending on their sanctioned strength and manpower position.

5.2.8.5 Non-verification of CPIS data by Treasury Offices

Treasury Officers are required to release salaries only to the employees whose names are reflected in the employee list supplied by the Nodal Officers. The Treasury Officers should verify the CPIS list downloaded from the website with the employees list submitted by the DDOs before releasing their salaries. They should not allow drawal of salaries of those DDOs whose employees data was not updated.

Also, an employee transferred and posted to another office/DDO shall not be allowed to draw his salary from the previous office/DDO from the date of issue of transfer order. His salary should be prepared by the new office/DDO by producing his Last Pay Certificate subject to updating of details of transfer by the DMIS.

The four selected treasury offices stated that employee lists were being enclosed by the DDOs as and when there was any change in the employee list due to transfer/posting, termination, retirement, *etc*. Further, it was stated that the employee list furnished by the DDOs were also being cross-checked with the transfer orders received by the treasury office.

Audit scrutiny in this regard, in the four selected treasuries revealed the following instances where treasuries had not exercised the required controls:

- 55 employees in the selected Departments had drawn their salary from the previous offices/DDOs after they were transferred.
- There were 75 employees in three offices *viz*., Deputy Commissioner (Chandel District), Nongmeikappam Gopal College (N. G. College) and Dhanamanjuri College (D.M. College) whose designations were upgraded due to their promotion but the same were not updated in the CPIS. Though CPIS did not have updated designation, the pay bills of these offices in which these employees were posted were still passed by the respective Treasury Offices.

- There were offices which had retired employees listed in their certified employee list. However, the pay bills (excluding retired staff) of these offices were passed by the treasuries.
- The Imphal West Treasury stated that they did not have User ID and Password to access CPIS website. Thus, the Treasury Office had no means to verify CPIS list submitted by DDOs before releasing the salary.

5.2.9 Security Controls

5.2.9.1 General Controls

General controls create an environment in which the application and application controls operate *e.g.*, IT policies, standards and guidelines pertaining to IT security and information protection. The general controls provide the foundation and build the control and security culture in an organization. Audit examined the adequacy of general controls in CPIS and audit observations are mentioned in the following paragraphs.

(a) Absence of IT Security Policy and Risk Assessment

An organization's formal IT Security Policy demonstrates its ability to reasonably protect business critical information and assets from loss, damage or abuse. It also aims to enhance the trust and confidence in the organization in addition to ensuring conformity to the mandatory regulatory requirements. IT Security Policy should be formal and future looking and should be based on the existing as well as future plans for use of IT in meeting organizational objectives and delivering the public services to the programme beneficiaries.

Further, since the threats and risks faced by the information systems differ from place to place and system to system depending on the various factors, it is imperative for an entity to assess and evaluate the risk environment and threats to its critical IT assets and processes so that the appropriate risk management strategies could be planned and carried out to bring these risks to an acceptable level. The risk management based on a formal risk assessment exercise is more effective and efficient if controls are placed at appropriate places based on need, thus, avoiding excessive controls.

The organization should also categorize its assets and processes based on their criticality and sensitivity, and the threats/risks to which they are exposed. The assets facing similar threats are grouped together for the purpose of risk management. While the risk assessment helps in efficient risk management, the asset categorization fosters economy by grouping similar assets together for risk management.

Audit scrutiny of IT Security Policy, Risk Assessment and asset categorization in the Directorate revealed the following:

- DMIS had neither prepared any formal IT Security Policy nor formally appointed any officer for the overall security in CPIS.
- DMIS had not done any formal risk assessment exercise to identify major threats to its IT assets and processes; system vulnerability to the threats;

likely business consequences in case the threats materialize, *etc*. Hence, the controls were on *ad hoc* basis created in CPIS.

- The Directorate did not maintain proper inventory of its assets (hardware and software) nor had it conducted any physical verification of its assets or classification of assets.
- Though maintenance of the CPIS database and server was entrusted to NIC, there was no documented formal agreement for the same.
- As NIC was maintaining CPIS, the DMIS was not aware as to how the database was being maintained or what security measures were in place for security of the database.

The Department, while accepting the audit findings, stated that they did not have any formal IT policy. The CPIS server and database were being maintained by NIC, Manipur, and they had their own IT policy. The reply was not acceptable since as an owner of the application, the Department should have its own formal Security Policy covering planning, development, management and business continuity of the applications.

(b) Ineffective IT Steering Committee

For successful implementation and operation of IT projects, there should be an IT Steering Committee comprising of user representatives from all areas of the business and IT personnel should be responsible for the overall direction of IT. The future direction agreed to by the IT Steering Committee is normally set out in a document known as the IT Strategic Plan, which should have approval of the top management.

Audit scrutiny revealed that though a Steering Committee was constituted in May 2013 under the chairmanship of Joint Secretary (Finance/Budget) to improve the existing work flow of CPIS by making CPIS management fully online and enhancing the scope of application of CPIS software but there was no representative from user Departments except Director, Treasury & Accounts, Manipur in the said Committee.

Further, only one meeting (May 2013) of the Committee was held so far (December 2018) which indicated that the role of the Committee was ineffective.

(c) Change management procedure

Change controls are put in place to ensure that all changes to application systems are authorised, tested, documented, controlled, systems operate as intended and that there is an adequate audit trail of the changes.

Directorate of MIS stated that they did not have any prescribed process for the management of changes in CPIS. There was no prescribed Form for Request For Change (RFC) or Control Register to log and monitor RFCs. Directorate also stated that changes to the software whenever done, were carried out by NIC after discussion was held between Finance Department and NIC. However, there were no documents in support of such discussion held in the past which resulted in the complete absence of audit trail to ascertain whether the changes sought for, were carried out successfully or whether such changes to the systems were approved by the competent authority.

The Department stated in response that there were only minor software errors and therefore, no official records of the changes made was maintained. The reply was not tenable as changes made in the software were required to be properly documented but such documentation was not done.

(d) Outdated Operating System and Antivirus software

CPIS application (client module) was installed on computers which has Windows XP as the Operating System (OS). Microsoft has already stopped providing software updates and security fixes for Windows XP that protect against malicious software, malware such as viruses and worms.

Two computers used in DMIS for updating CPIS were test checked during audit and it was found that these computers had security patches upto 15 May 2017 making them vulnerable to security threats that had originated after that date.

Audit also found that the antivirus software (Quick Heal) installed on the two test-checked terminals had virus definitions updated till 30 March 2018 and 16 February 2018 respectively.

The Department stated in reply (December 2018) that the NIC used to update antivirus from time to time. The reply was not tenable since updating of the operating system and antivirus was the responsibility of the system owner *i.e,.* DMIS, which was not done periodically, making the system vulnerable to virus and worms that originated after the aforesaid dates.

(e) Environment Controls

Environment controls are aimed at ensuring that the application system and IT assets are not put to risk due to fire/water damage or damage from other natural disasters, earthquakes or failure of equipment due to extreme temperature or humidity, *etc.* The preventive measures should be based on results of a formal risk assessment exercise.

Audit found that DMIS was housed on 3rd floor of the New Secretariat Complex in Imphal. The Directorate had not undertaken any formal risk assessment to assess the possible environmental threats to CPIS. The smoke and fire detection equipment, fire extinguishers, water detectors, *etc*., were not in place in DMIS. However, there were two fire extinguishers installed nearby but it was observed that both had already expired on 01 March 2012. Hence, DMIS had no basic measures like fire extinguishers for the last six years. No mock drill for fire and earthquake safety was found to be carried out by DMIS. There was also no Uninterrupted Power Supply (UPS) available for the computers at DMIS.

It was further observed that in addition to the IT equipment, DMIS also had loads of important files (hardcopies) which were kept scattered and piled up in the data entry room and godown. This was serious keeping in view the lack of basic environmental security measures in DMIS. This could lead to loss of important files (hard copies) and destruction of properties in the event of any fire incident.

Audit also observed that the CPIS server was housed in the Data Centre located on the ground floor of the New Secretariat complex. The location of the server on the ground floor makes it more vulnerable to threats like flood, rains and theft.

Photograph No. 5.2.1 Lack of disaster preventive measures

DMIS office with no CCTV camera, fire extinguishers, smoke sensors etc. (19 September 2018)

Files in the DMIS room with no fire extinguishers, smoke sensors, etc. (19 September 2018)

Source: Audit documentation of DMIS.

The lack of appropriate environmental controls could lead to system unavailability, thereby affecting CPIS objectives adversely. The Department accepted the audit findings and replied that they would strengthen environment controls in future.

(f) Physical Access Control

Though security personnel were stationed at the main entrance of the Secretariat complex, the DMIS rooms where CPIS data entry/updating work was being done, was easily accessible to the visitors coming to the building complex without any restrictions. Records about the visitors' entry were not maintained in DMIS. No burglar alarm system or CCTV camera was found installed at DMIS for monitoring and security of the DMIS rooms, records, *etc*. The absence of appropriate physical access controls could increase the risks of loss/tampering of important documents and damage to the systems.

The Department, in response to an IT Audit Report (Paragraph 1.2.11.11 of CAG's Report 2010) had earlier stated that restrictions had been imposed on the entry into the rooms of data entry operators and log of visitors were being maintained. However, neither any restriction was in place on entry into DMIS nor any visitor's log or record was found to be maintained in DMIS even after a lapse of eight years, thereby putting CPIS to a big risk.

(g) Logical Access Control

The organization should have a documented process on access control to ensure segregation of duties; reviewing users' privileges to ensure that it conforms to the job needs and security requirements; establish suitable process for users' registration/ de-registration and a policy supported with a set of guidelines/best practices on selection and use of good passwords. Access controls also require appropriate configuration of log files and their periodical review to monitor the security concerns; controlled access to the application source codes; and also the installation and appropriate configuration of firewall, routers and intrusion detection and prevention system (IDPS) to secure the information systems from the external threats. The audit scrutiny of IT Access controls revealed the following:

Weak Users' Management

The Department did not have formal documented user registration and de-registration process for managing and controlling users' access to CPIS. Audit found that there were 45 recorded User IDs in CPIS and out of them, 20 users were inactive while the remaining 25 were still active. The active User IDs includes One "Super" User ID; two "Admin" User IDs; four "Data Manager" IDs and 18 "Computer Operators" IDs. However, the Directorate had only one Director, one Under Secretary (Finance), one System Manager, one Computer Programmer and seven Computer Operators. Since there are only 11 Users in DMIS, the number of active User IDs exceeded the staff posted at DMIS, thereby endangering CPIS with the possible unauthorized access to the system.

Absence of Password Policy

An organization should have a formal Password Policy and guidelines mandating periodical change in passwords, composition of passwords, minimum and maximum length of password, not-sharing of passwords, *etc*. It was, however, observed as under during audit:

- DMIS had neither any formal Password Policy nor any set of guidelines containing best practices on passwords.
- CPIS neither enforced nor asked for password change when a user logs in, for the first time.
- There was neither any prescribed minimum and maximum length for passwords nor was any prescription for the password composition (alpha, numeric, symbols, *etc*.) mandated by the CPIS system.
- There were no restrictions on number of login attempts to prevent unauthorised access through guessing of the passwords and making repeated failed access attempts.
- Although each Nodal Officer had different user ID and password, they were sharing their passwords with their subordinate staff.
- In many cases, when a staff member had been transferred, his/her user ID and password was still retained without being deactivated.

Absence of Password Policy or guidelines mandating composition and use of strong passwords in addition to controls ensuring good practices in use and management of passwords, puts the system to high risk, thus, endangering the confidentiality, integrity and availability of system.

The Department, in response to an IT Audit Report (Para 1.2.11.12 of Audit Report 2010) had earlier stated that they would consider having a formal password regulation in respect of CPIS. However, no records in support of creation of any formal password regulation in respect of CPIS was produced to Audit despite specific request made by Audit in this regard.

Weak Logical Access Control

Audit scrutiny revealed the following weaknesses in respect of logical access control:

- CPIS allowed a user to be logged-in on two computers simultaneously, thereby ignoring concurrent session control.
- CPIS allowed two users to log in simultaneously on the same Computer thereby, making possible for a user to use the account of the other user in an unauthorised manner. The data entry and its verification at the same time using same terminal was possible due to the absence of this control.
- There were no restrictions on the number of login attempts to prevent unauthorised access through repeated hit-and-trial attempts.
- The System did not log off users even after it was left unattended for some time to prevent unauthorised access.

The above shortcomings were indicative of weak logical access control in CPIS. These weak logical access controls coupled with the weak physical access controls made the system vulnerable to the risk of unauthorized access, amendments or deletion of data and consequent losses.

(h) Business Continuity and Disaster Recovery Plan

Business Continuity Plan, Disaster Recovery Plan and data backup policy prescribing backup time table, backup process, life time of media and responsibility to take regular backups, test backups and to restore data are necessary for recovering key business processes in the event of a disaster. The objective is to reduce downtime and minimise loss to the business in the event of disaster taking place.

Audit found that DMIS was not having any formal Business Continuity Plan, Disaster Recovery Plan or Data Backup Policy. The Department had also not organized any awareness campaigns during 2016 to 2018 to make staff members aware of the importance of the periodical backing up of their data, information and applications. Audit noticed that no special training for the staff members who were to play key roles in the disaster recovery operation was conducted in DMIS.

On this being asked by Audit, the System Manager at DMIS stated that they take both full as well as incremental backups using the backup module available in CPIS and the backup is stored on the Storage Area Network (SAN) of the Manipur State Data Centre. During the physical inspection (23 October 2018) of CPIS backup at the Manipur State Data Centre, it was found that Full backup of CPIS was last taken on 16 October 2018. However, no incremental backup was taken for the next seven days after taking the full backup.

The Department had also stated that NIC regularly backed up data in tapes and kept the same in an offsite location at NIC office. However, during physical verification of the site, it was observed that the data had not been backed up since September 2018 due to a defective fibre cable switch. Further, no copy of CPIS backup was found kept in an offsite location.

Besides, the backed up data and application were not tested to see whether it would actually work in case of any such eventuality. Thus, there was no certainty that the backed up data and application would work as it had not been tested.

Recommendation (23): DMIS should conduct formal risk assessment exercise to identify possible risks and should develop formal policies on IT Security, Access, Passwords, Business Continuity, staff development, etc., and ensure their effective implementation.

5.2.9.2 Application controls

Application controls are specific to an application which seek to minimize the risk of incorrect and incomplete data entry by making validation checks, duplicate checks and other related controls. These provide the earliest opportunity to detect and correct possible mistakes, and thus these controls are vital to the integrity of a system. The organization should have formal procedures and controls in place to ensure that all transactions are authorized before being entered into the Computer system. Following issues relating to lack of application controls were noticed:

(a) Age less than 18 years on Entry into Service and Date of Entry into Service earlier than the Date of Birth

As per prevalent rules for recruitment into Government service, a minimum age limit is prescribed and the software should have inbuilt embedded controls to reject those entries which did not fulfil the minimum age limit criteria. CPIS has input control for entry of employee whose age is less than 18 years. However, on analysis of the database, it was observed that:

- 863 out of 78,195 employees had joined service before attaining the age of 18 years;
- Out of these 863 employees, 21 had their date of joining even before their date of birth and nine employees had date of birth same as their date of joining; and
- Seven employees were shown to have joined Government service on future dates (2019 to 2027).

The Department, in response to an earlier IT Audit Report (*Paragraph 1.2.11.16* of CAG's Audit Report for the year ended 31 March 2010) had stated that the mistakes were made during the data entry into MGEL project and these incorrect data were being rectified. However, even after eight years since the last audit, the Department was yet to verify and correct the CPIS data.

Regarding the validation checks for employees under 18 years of age, the Department stated that these were not done at the time of MGEL. However, after the implementation of CPIS application, there was a proper validation check for employees under 18 years of age. The reply was not acceptable as

CPIS data contains employee details which proved that the validation checks were not effective and thus, needed strong inbuilt application controls in the system.

(b) Men-in-position exceeding the sanctioned strength

One of the objectives of CPIS was to restrict posting of employee in excess of the sanctioned posts. The system should have embedded controls to reject any data entry of the employees in excess of the sanctioned strength.

Audit analysis of CPIS data related to the four selected Departments *viz.*, Education (S), Medical and Health Services, Commerce and Industries and PWD revealed as under:

- There were 140 employees in-position against the sanctioned strength of 80 pertaining to different posts in 22 of their offices. As such, there were 60 excess employees over and above the sanctioned strength.
- There were 287 employees of different categories in 63 offices of PWD for which there were no sanctioned posts.

The Department stated that men in position exceeding the Sanctioned strength occurred at the time of MGEL. After the implementation of CPIS, sanctioned post validation was done by the application before updating. In case of the engineering Departments, the excess strength was due to employees having been converted to regular from work-charged, which was a dying post once the work charged converted employee retires. The reply was not acceptable in audit as the CPIS data was itself reflecting the men-in-position that exceeded the sanctioned strength, depicting the ineffectiveness of application controls of CPIS.

(c) Lack of controls on forms received for updating CPIS

DMIS must have a monitoring mechanism to ensure that all the input documents/forms received from the Department are immediately posted/updated in CPIS and that no input document/form is lost or left out.

Audit found that the Directorate has provided a drop box where CPIS forms/inputs are dropped by the user Departments. The forms are serially numbered after taking out from the drop box and then entered in a register. However, except for the Department of Education (S), details of the forms, *viz.*, names of the employees, form number, date of sending of forms, *etc*., were not found mentioned in the register by various Departments. As no receipt/acknowledgment number is issued to the Departments, there is always a risk of loss of forms. Further, there was no system existing in DMIS to ensure that all the forms received have been keyed into CPIS.

(d) Mismatch of Title and Gender

The title (Shri, Smt. *etc*.) of an employee is determined by the gender (Male/Female) of the employee. There was no embedded input control in CPIS to ensure that only such title for a male or female was assigned to an employee according to his/her gender. On an analysis of the database, it was observed that the titles of 1640 employees were found to be contrary to their gender.

(e) Existence of Basic Pay less than the minimum entry pay

CPIS application should not allow basic pay of an employee to be less than the minimum entry pay for the posts. On testing of the input controls, it was found that CPIS does not validate Basic Pay against the minimum of the pay scale and it accepts any lower value than the minimum of the pay-scale. Further, analysis of pay details of 5,660 employees who had joined service between April 2013 and March 2018 revealed that 3,224 of them had Basic Pay less than their respective minimum entry pay of the post.

(f) Incorrect employee details

For any information system to achieve its objectives, it is necessary that suitable input controls are put in place to ensure that the information captured by the system is correct and complete. Audit analysis of CPIS data revealed the following errors:

- Name of 160 employees in 29 selected offices as per service records were not matching with those in the CPIS database.
- In seven Departments[162], 15,814 employees have numbers as part of their names.
- Date of Birth of 58 employees out of 343 in 22 selected offices as per service records were not matching with those in the CPIS database.
- Date of Joining of 43 employees in 11 selected offices as per service records were not matching with those in the CPIS database.
- Out of 78,195 employees in CPIS database, 9,928 did not have title in their names and 170 employees did not have father's name mentioned in the system.

(g) Delays in CPIS updating on recruitment, promotion, transfer, *etc*.

Updating of CPIS is a continuous exercise and it is pertinent that the input forms are quickly sent by the User Departments to DMIS and DMIS promptly keys in and updates CPIS database. The system should have in-built controls to prompt non-entering of data and should be able to generate feedbacks to cross-check delays of data entry. Audit, however, found that there were inordinate delays by the User Departments and DMIS in sending input forms and updating the data in CPIS respectively and also there was no mechanism devised in the system to prompt/give feedbacks such delays as is evident from the following details:

- In the case of 53 out of 55 newly recruited employees of four[163] selected Departments, the delay in issue of EIN ranged from one to 44 months.
- In the case of 71 out of 72 test checked employees of four[164] selected Departments, employees' data on account of promotion was not updated

[162] Excise, GAD, Home, Power, Revenue, Vigilance and Youth Affairs & Sports.

[163] Agriculture, Assembly Secretariat, Forest and Revenue Department.

[164] Agriculture, Veterinary & Animal Husbandry, Forest and Home Department.

in a timely manner and the period of delays ranged from one month to eight years.

- Due to inaccuracy in the date of birth captured in CPIS, the details of retired employees were not found removed by DMIS; rather they waited for the submission of forms from the concerned Nodal Officers. Consequently, data of many retired employees were present in the database. Delays ranging from one month to five years were noticed in updating of the termination forms in all 239 test-checked cases of employees belonging to 12[165] selected Departments.
- In the cases of organized services, it was found that in the selected DDOs, details of the 28 out of 49 officers present in the employee list (September 2018), were not updated. Further, the details in respect of 17 officers who were posted and working in the selected offices, were not found reflected in CPIS. Test check of forms of selected Departments in the Directorate of MIS further revealed that updating of data of the officers of Organized Services was delayed up to five years.
- In the case of 24 out of 25 test checked employees who were transferred and belonged to six[166] selected Departments, it was found that the delays in updating data ranged from one month to 18 months.

Thus, due to the inaction/delays in submission of inputs by the Departments and updating by DMIS, the CPIS database was not accurate and reliable causing inconvenience to the employees concerned in addition to compromising the usefulness and effectiveness of CPIS. The above deficiencies noticed by Audit confirms that Application Controls in the system were weak as it allowed entry of non-relevant data and it failed to prompt delays in data entry.

The Department accepted the above audit findings and agreed to carry out risk assessment to assess the possible risks to CPIS/CMIS system so that the controls are based on risk assessment. The Department also agreed to strengthen the physical and environmental controls and also to formalize a change management procedure. The Department also agreed to streamline the process of access to the system and to develop formal policies relating to business continuity, Access Policy, Password Policy and Security Policy in addition to incorporating suitable application controls in CMIS before rolling out.

Recommendation (24): DMIS should devise suitable controls duly embedded in the software to minimize the entry of erroneous data in the system so as to ensure integrity of the CPIS data.

Recommendation (25): The audit findings and recommendations may be kept in view while developing CMIS replacing CPIS by the Government.

[165] Forest, Commerce & Industries, Home, Command Area Development Authority, State Academy of Training, Public Works Department, Agriculture, Education (S), Education (U), Veterinary & Animal Husbandry, Assembly Secretariat and Revenue Department.

[166] Forest, Agriculture, Command Area Development Authority, State Academy of Training, Public Works Department and Veterinary & Animal Husbandry Department.

5.2.10 Monitoring and Supervision

5.2.10.1 Lack of monitoring

Involvement of the senior management in development and management of CPIS was found to be deficient. There was over reliance on NIC for system maintenance and backups even after DMIS, Finance Department had taken over the overall responsibility for CPIS in January 2010.

Senior management develops and approves the strategy and policy documents to ensure that the IT operations meet the organizational objectives. However, Audit found that DMIS did not have appropriate IT Strategy, IT Security Policy, Access Policy, Password Policy, Business Continuity Plan, *etc*., for ensuring the effectiveness of the CPIS.

Management has the ultimate responsibility for ensuring that an adequate system of internal controls is in place to seek assurance about the effectiveness of controls through the review work carried out by the internal auditors. However, CPIS did not have Internal Audit mechanism in place.

Management supervision and monitoring of data entry was absent as evident from the large number of incorrect/improbable data of the CPIS. The generation of a sizeable number of rejected forms each month and inordinate delays in submission of input forms across almost all the Departments showed lack of monitoring and inadequacy of controls.

On the above being pointed out, the Department stated in response that necessary action would be taken to strengthen the monitoring and supervision of CPIS/CMIS. However, they also added that only the operational part of CPIS had been taken over by Finance Department from NIC in January, 2010 but for the technical issues, CPIS database and server were still being maintained by the NIC, Manipur. As such, NIC has its own IT Security and Access policies.

The reply was not acceptable as the senior management being the owner of the applications, should be more proactive and come out with their IT policies for meeting the intended objectives through CPIS.

Recommendation (26): To ensure that CPIS/CMIS meets its objectives, senior management may take the lead by formulating suitable policies for their implementation.

5.2.10.2 Non-availability of Helpdesk

Help Screens/desks are the day-to-day link between users having IT problems and the IT Department. They are the respondents to users call to resolve any problem in relation with the system. Dedicated staff has to be allocated for attending any requirement that comes at the help desk. However, there was neither any helpdesk in the DMIS office due to lack of manpower nor any help screen available at the CPIS website to address the related issues.

5.2.11 Audit Constraints and Limitations

IT Audit of CPIS commenced with holding of an Entry Conference (April, 2018) wherein the officials of Accountant General (Audit), Manipur, Directorate of MIS and NIC, Manipur were present. Though Audit had requested for CPIS database in March 2018, the Department provided incomplete/partial database (12 MB in MS Excel out of 1.5 GB) in August 2018 after a lapse of four months. Similarly, documents and replies to the audit queries requisitioned (April 2018) by Audit were provided by the DMIS after a delay of four months.

Due to lack of complete database, Audit could not analyse the database completely and thus, could not comment on employee history and transaction log for changes made in employee details and sanctioned post details (date of data entry and data verification, data entered by, data verified by, sanctioned post abolished order number and date) *etc*.

5.2.12 Conclusion

The CPIS application was developed with a view to providing accurate details of the staffing pattern of the Government employees, capture details of employees to facilitate policy decision on deployment, redeployment and transfer of employees, estimate budget for salaries, *etc*., and thus to help the Government in proper administration. However, the CPIS was developed without obtaining URS resulting in lack of provision for capturing full employees' details limiting the usefulness of the system. The existing CPIS was being used to a very limited extent for preparing salary bills. However, it was not being used effectively for transfer and posting of the Government employees as envisaged.

The usefulness and effectiveness of CPIS had been significantly compromised by inaccurate and incomplete data imported into CPIS from the erstwhile MGEL application, inordinate delays in sending input forms by DDOs, weak input controls, non-existent IT policies, lack of staff development and succession planning, lack of business continuity measures, absence of involvement of senior management, *etc*. It also exposed the system to the risk of unauthorised access, amendments or deletion of data and consequent losses.

There were employees who had crossed the age of retirement but were still being shown in the CPIS database which defeated the objective of CPIS to provide accurate staffing pattern of employees. The lack of correct employee details also defeated the intended objective. Moreover, the CPIS was also not being used for the intended purpose of proper deployment of the staff to various offices.

HOME DEPARTMENT

5.3 Non-realisation of security charges for armed guard

Failure of the Department to enforce provisions of Government's decision for recovery of armed guard charges from seven banks resulted in non-realization of security charges of ₹ 1.47 crore, of which ₹ 31.24 lakh had been recovered.

According to Rule 12 of General Financial Rules, 2005, amounts due to Government shall not be left outstanding without sufficient reasons. As per a decision (May 2000) of Government of Manipur, armed guard charges[167] for providing security arrangements were to be deposited into the treasury by the banks concerned. Non-payment of the amount was also liable to invite penalty equivalent to the arrear amount.

Scrutiny of records[168] (May 2017) of the office of the Director General of Police, Manipur revealed that the charges for armed guard for deployment of security personnel to seven banks for periods ranging from March 2013 to March 2018 were not paid by the banks as of June 2018 as shown in the following table.

Table No. 5.3.1 Details of outstanding armed guard charges due from defaulting banks as of June 2018

(₹in lakh)

Sl. No.	Name of defaulting banks	Period of default	Outstanding armed guard charges
	State Bank of India		
1	Gamnom Saparmeina branch, Kangpokpi	March 2013 to March 2018	15.64
2	Mayang Imphal branch, Imphal West	April 2013 to March 2018	9.60
3	Moreh branch, Tengnoupal	September 2013 to March 2018	12.43
4	Singjamei branch, Imphal West	March 2014 to March 2018	8.87
5	Wangoi branch, Imphal West	March 2014 to March 2018	10.38
6	Thanlon branch, Pherzawl	February 2016 to March 2018	15.60
	United Bank of India		
7	Senapati branch	June 2016 to March 2018	0.75
	Total		**73.27**

Source: Departmental Records.

On being pointed out by Audit (May 2017 and August 2017), the Department intimated (September 2017) that the defaulting banks had been instructed to clear the outstanding dues. Audit, however, observed that the banks had not cleared their dues which worked out to ₹ 73.27 lakh as on June 2018. Despite provision of withdrawal of security personnel for non-payment of armed guard charges for three consecutive months in the State Government decision *ibid*,

[167] ₹ 2,000 per personnel per month, as per letter No.3/5(1)/2000-H of Home Department, Government of Manipur dated 30 May 2000, which was further increased to ₹ 5,000, as per various notices issued between October 2012 and January 2016.

[168] With further information provided by the Department (June 2018).

the Department failed to take concrete action to withdraw security personnel or to ensure recovery of outstanding dues of ₹ 1.47 crore *(Armed guard charges - ₹73.27 lakh and Penalty - ₹73.27 lakh)* from the defaulting banks for a period[169] ranging from two years to five years and three months.

Thus, failure of the Department to enforce provisions of the Government's decision for recovery of armed guard charges from the seven banks resulted in non-realization of security charges of ₹ 1.47 crore.

On this being pointed out, the Police Department stated (October 2018) that a list/statement of defaulting banks for non-payment of armed guard charges had been furnished to the Administrative Department for the further course of action. The Police Department further intimated (February 2019) that an amount of ₹ 31.24 lakh had been recovered[170]. Thus, an amount of ₹ 1.16 crore was still outstanding for recovery from the defaulting banks.

It is recommended that before providing armed guards, the Department should consider for entering a Memorandum of Agreement with the banks concerned to obviate such a situation in future.

[169] As reckoned upto June 2018 *i.e.,* the month in which the matter was pointed out.

[170] The name of banks from which the amount had been recovered, was not furnished.