* ~~Annual Action Plans should be prepared timely after ascertaining and prioritizing the requirements of each village through VDBs and emphasis should be on creation of durable assets.~~

* ~~Basic records like muster rolls, employment registers and asset registers should be maintained.~~

* ~~Funds should be released on time at various levels and the State Government should release its matching share for successful implementation of the programme.~~

* ~~There should be proper accountal of foodgrains allocated, lifted and distributed and records relating to these aspects should be reconciled at various levels at regular intervals to plug loss/pilferages.~~

* ~~Proper mechanism should be instituted for monitoring the implementation of the programme.~~

~~The findings were reported to the Government in August 2007; reply had not been received (November 2007).~~

ELECTION DEPARTMENT

3.3 Information Technology Audit of Electoral Roll and Voter Registration System

The preparation and updation of electoral database is the responsibility of Chief Electoral Officer. The Department took up Intensive E-Roll (Electoral Roll) revision in 2004 in all the districts of Nagaland as per the instructions of the Election Commission of India (ECI) and completed it in 2005. Audit examination of the E-Roll system revealed deficiencies in security, access, input, and backup controls resulting in unreliable data.

Highlights

The Department is yet to formulate an IT Policy, even though computerisation of Electoral rolls is about a decade old.

(Paragraph 3.3.7.1)

No documentation exists for Electoral Management System; periodical modifications made to the system were not documented.

(Paragraph 3.3.7.2)

The Department spent Rs.3.10 crore for issue of Electoral Photo Identity Card (EPIC) – but the E-Roll database could not be synchronized with the EPIC database

(Paragraph 3.3.7.4)

Defective manuscripts coupled with lack of controls to detect duplications and inconsistency in details of voters at the district level (during electoral enumeration) and State level (during data entry and processing) resulted in

defective electoral data. Inadequate input and validation controls resulted in duplication of data in electoral rolls and unreliable data.

(Paragraph 3.3.7.5)

Inadequate physical and logical access controls make the system susceptible to security breach, data theft/ manipulation and induced breakdown. The System was also infected with virus.

(Paragraph 3.3.7.6)

The Department does not have a back up policy and disaster recovery procedures.

**(Paragraph 3.3.7.7)**

3.3.1 Introduction

Under Article 324 of the Constitution, the superintendence, direction and control of the preparation of electoral rolls for, and the conduct of, all elections to the Parliament and to the Legislature of every State, and elections to the offices of the President and Vice-President are vested in the Election Commission of India (ECI).

At the State level, the election work is supervised, subject to the superintendence, direction and control of the ECI, by the Chief Electoral Officer (CEO) (appointed by the ECI) and the officers and staff working under him.

At the district level, the election work is supervised, under the direction and control of the CEO, by the District Election Officer (DEO), who is generally the Deputy Commissioner of the district. The Deputy Commissioner is also designated as Electoral Registration Officer (ERO) and is responsible for preparation and maintenance of Electoral Rolls.

Computerisation of Electoral Rolls in the Department began during the 1990s. Since then, the system has undergone several changes. The Department took up Intensive E-Roll (Electoral Roll) revision in 2004 in all the districts of the State under the instruction of the ECI, and completed it in 2005. The present E-Roll system is based on the Intensive Revision of 2005 and updated upto 1 January 2006.

3.3.2 Organisational set-up
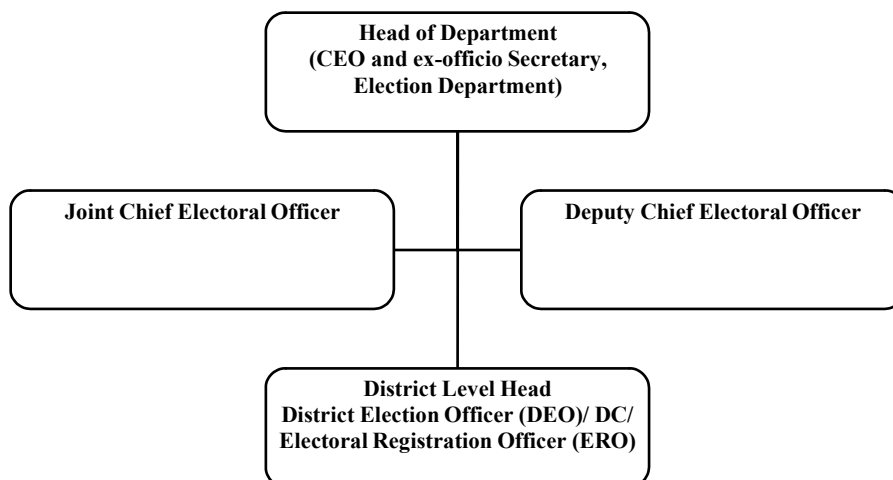
3.3.3   Overview of the System

The computerized E-Roll system is located primarily in the office of the CEO at Kohima. The system comprises 2 servers running on Linux, housing the E-Roll database, and 7 Windows based desktop computers. While the E-Roll database is in MS Access format, Visual Basic is the front-end tool.

The processes involved in the system and data flows are summarised below:
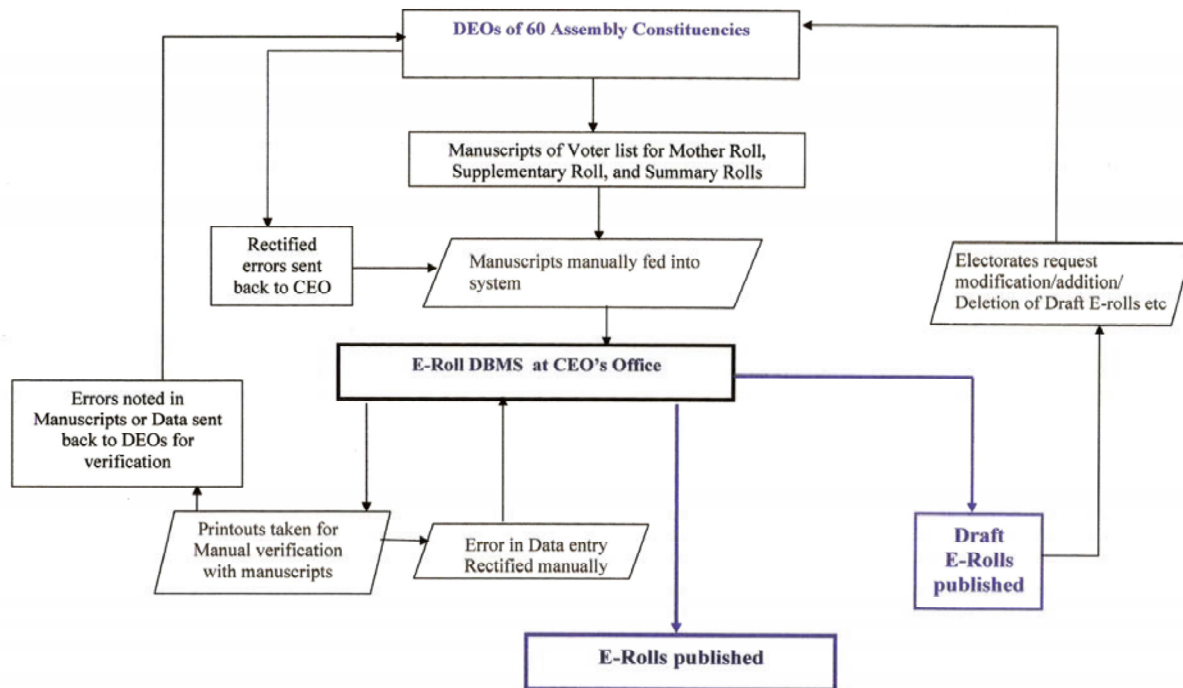
There are about 1243143 registered voters in Nagaland as on 1 January 2006 (as per the E-Roll System) spread over 11 districts, 16 Assembly Constituencies and 1563 polling stations.

3.3.4   Audit Objectives

The main objective of the IT audit of the E-Roll System was to see whether the primary objective of the Department to have an error-free Electoral Roll had been achieved. For this purpose, audit had to:

∗   Analyse the E-Roll System for the completeness, integrity, reliability and accuracy of the data, and the adequacy and effectiveness of controls.

∗   Evaluate the security of the system.

∗   Evaluate the back up and disaster recovery procedures for the system.

3.3.5   Audit Scope and Methodology

IT audit of the E-Roll system was conducted in July 2007 through an analysis of the data in the system, and the related manual records, policies and procedures. For this purpose, the data in the E-Roll system was downloaded, and analysed using SQL queries.

3.3.6   Audit Criteria

The guidelines and instruction of the ECI issued to the CEO from time to time in respect of Summary Revision 2000 and Intensive Revision 2005 were used as audit criteria.

Audit Findings

The major findings of IT audit are summarized in the succeeding paragraphs.

3.3.7   System Implementation

3.3.7.1 Lack of IT Policy

While computerization of electoral rolls started about a decade ago, and the Intensive Revision of electoral rolls was conducted in 2004, the Department is yet to formulate an IT policy for proper governance and control of its IT activities. Currently, there is just one IT-literate person in the CEO's office, who manages all aspects of the system.

3.3.7.2 Lack of Documentation

The software used for the E-Roll system viz., "Intensive Revision Version 1" is a modified version of the software originally provided by ECI for Summary Revision 2000. The ECI provided the source code with complete system documentation to the CEO for customization as appropriate, keeping in view the existing database of the Department. During Intensive Revision 2005, the Department outsourced the development of software to a private firm (M/s Nagasoft Kohima), which had been appointed as the advisor to the CEO for all IT-related activities of the Department. There was no System Requirement Specification (SRS) or System Design Document (SDD), as a result of which, development of the system was done in an ad hoc manner. The modifications made to the existing source code and database were not documented; consequently, vital controls required for data integrity and validation were not incorporated, resulting in invalid and inaccurate data, as brought out in the succeeding paragraphs. Further, the Department had made several changes to the software since its commissioning but there is no documentation relating to such changes to the system or any trail within the system to indicate the changes.

3.3.7.3 Undue advantage to SLA

As per the instructions of ECI, the Department appointed M/s Nagasoft Kohima as the State Level Agency (SLA) as professional advisor to CEO on all IT related activities of the Department initially at an amount of Rs.5000 per month, enhanced to Rs.7500 per month latter. Apart from providing advice on professional matters, the firm was also entrusted with other IT related functions like data entry and printing of E-Rolls,

supply of hardware and stationery, development of software for printing photo identity cards etc., for which an amount of Rs.52.39 lakh was paid apart from a professional fee of Rs.5.22 lakh.

However, the firm could not develop a robust system for Electoral Rolls that conforms to the guidelines issued by the ECI. Also the firm could not advise the CEO properly on the rights of the Department with regard to the Electoral Photo Identity Card (EPIC) database and software.

3.3.7.4 EPIC Database

The Department engaged M/s. Eastern Printers, Mokokchung at a cost of Rs.3.10 crore for developing the software necessary for capturing the photograph of the voters and printing and issuing laminated Photo Identity Cards with the hologram. The firm was also required to supply miniaturized identity card, pouch laminated in tin durable fine sheets of A4 size containing 100 miniature cards. A unique ID No. for every voter in the format prescribed by the ECI was to be generated and the application alongwith the manuals were to have been handed over to the CEO.

Audit scrutiny of the EPIC database revealed that the details of voters for whom EPIC was issued and database with the photographs of the voters were not made available to the Department by the firm. There was also no synchronization between the E-Roll and EPIC databases.

3.3.7.5 Control Environment

The DEOs get the manuscript of the electorate enumerated by officials like BDOs etc., which forms the basis for the data that is fed into the E-Roll system. The DEO/officials nominated by the DEO, are to personally verify the information furnished by the voters and ensure that it is correct before the manuscripts are passed on to the CEO for entering the data in the system. While the Department informed audit that 100 *per cent* verification of the print outs is carried out and reconciled with the manuscripts, audit analysis of the data revealed that the input controls and validation checks in this regard were very weak leading to numerous duplicate records, as detailed below:

∗   There were 5877 records in the system where the name of voter, assembly constituency, polling station and house number were identical;

∗   There were 3636 records where the name of voter, assembly constituency, name of father/husband and house number were identical, irrespective of the polling station;

∗   There were 3277 records where the assembly constituency, name, name of father/husband, sex and age were identical;

∗   Female voters were categorized as 'M' (Male) in the database. In fact, the system accepts Sex field as 'M' (Male) when the Father/Husband relationship field is shown as 'Husband';

∗   The system did not capture any records in the field 'LASTNAME'; instead, the first name and last name of the voters were clubbed together in the field 'FM_NAME', resulting in capturing of short name of electors in single field as shown below:

* There were 11,48,117 records out of 12,43,143 where only the first or the second name of the voter were captured;

* There were 28,000 records with only the short name. Examples are given below:

Examples of records where only first or second name was captured	Examples of records where only short names were captured
Dilip	A. Kalam
Asenla	P. Khathsen
Achila	T. Kiusu
Chandeshwar	T.L. Phankiu

Considering that there could be many voters with similar names, unless the full name including the first, middle and the last name of the voter is captured, there will be confusion with regard to the names and consequently, the possibility of one voter passing off in the name of another voter, who has the same first/last name.

The Department accepted (September 2007) the audit observation and agreed to take necessary corrective action.

There were also numerous instances which point to weak validation controls in the system. Some such instances are given below:

* The system accepts any number from 18 to 999 with regard to the age of the voters; there were 274 records where the age of the voter was recorded as above 100.

The Department accepted (September 2007) that only the lower age limit was specified in the system and stated that the upper age limit was not yet programmed.

The ID Number field was incomplete and did not conform to the format specified in the ECI guidelines. While the ECI guidelines stipulate 7 digit Unique ID for the electorate, audit analysis of the data revealed the following:

* Only 10814 out of the 12 lakh records were provided with 7 digit ID No. and out of this, only 3459 records conform to the format prescribed by ECI. The remaining 7355 out of the 10814 records, are appended with wrong check sum (Check sum number is a part of the 7 digit ID Number, the format prescribed by ECI).

* There were 171219 records where the ID No. was not given; 770 records with duplicate ID No; 18 records with triplicate ID No. and 2 records with quadruplicate ID No.

* There were 285 records with less than 6 digit ID No. and there were 3028 records with invalid characters like comma, asterisk, hyphens, alphabets, leading spaces, etc.).

As detailed above, despite the Department claiming that 100 *per cent* verification of the manuscripts and reconciliation between the manuscripts and the print outs was being done, there were numerous cases of invalid and inaccurate data due to poor input and validation controls in the system.

3.3.7.6 System security

∗ **Physical access controls**

Physical access controls are necessary to ensure that only those people who are authorised by the Department have access to the system. Audit scrutiny revealed that the system including the servers, network switchers, etc., were freely accessible to any user in the Department making it vulnerable to physical threats.

∗ **Logical access controls**

Logical access controls are important to ensure that only authorised users log in to the system and have specific access rights to the functions that are relevant to them. It was observed that the data entry operators log in to the system using common user name and password and have access to all the folders, files and menu options in the application and can add/delete/modify the records in the database. In fact, the database is not protected by passwords and any user can access it and can append/modify/delete the records or the database itself. There are no system or audit logs to identify the users who have accessed the system or made changes to the data in the system.

∗ **Antivirus software**

It was also noticed in audit that the system was infected with virus. Although the Department had an antivirus software, its license had expired and the Department had not taken any action to renew the license to ensure that regular updates for the antivirus software are received.

The Department accepted (September 2007) the audit observations and agreed to take necessary corrective action.

3.3.7.7 Back up and Disaster recovery procedures

The Department does not have a policy for backing up the database, which is very critical to its functioning. Although there is an external hard disc for back up purposes, the data is not backed up at regular intervals nor are the backups stored at a different location to ensure continuity of operations in case of any disaster in the server room/building/location.

The Department does not also have a disaster management policy to ensure that the system is operationalised quickly in case of any disaster. In fact, there is no fire prevention or detention facility in the computer lab.

The Department accepted (September 2007) the audit observation and agreed to take necessary corrective action.

3.3.8 Conclusion

The implementation of the E-Roll system was not systematic and did not take into account the specific requirements of such a mission critical system, which is of immense importance to the conduct of elections and exercise of franchise by the electorate of the State. Poor input and validation controls have led to duplicate and invalid data in the system and the security of the system, both physical and logical

access, is very inadequate to guarantee the confidentiality, integrity and availability of the data. Lack of back up policy and disaster recovery procedures make the system vulnerable and incapable of recovering the data in case of unforeseen disasters/contingencies. In a democratic set up, where every single vote is significant, the importance of setting up an error free E-Roll system cannot be over emphasized.

3.3.9 Recommendations

The following measures are recommended to ensure adequate security to the system and confidentiality and integrity of the data contained therein:

* The Department needs to formulate an IT policy to ensure that IT systems are developed and operated efficiently and effectively to achieve the objectives of the Department.

* The system needs to be documented and all the changes made to the system have to be carefully considered, authorised and documented.

* Adequate input controls should be built into the system to ensure that only valid data is fed into the system. The Department needs to review the data immediately and ensure that all invalid, duplicate and junk data is deleted.

* Antivirus software should be procured, installed, updated and run on a regular basis to ensure that data is free from virus.

* Only authorised personnel should have access to the computer lab which may be ensured through the use of smart cards etc.

* Password policy should be framed and enforced so that only authorised users have access to the system/folders/files on a need to know basis. Audit logs should be activated and reviewed at regular intervals to ensure that unauthorized activities do not go unnoticed.

* There should be a clear back up policy and regular backups should be taken, stored offsite and tested periodically to ensure that these can be used when required.

* Considering the criticality of the system, the Department should formulate and document a disaster recovery plan and test it to ensure that the staff is aware of their responsibilities in case of a disaster and the system is operational within a specified period after any disaster.

HOME (POLICE) DEPARTMENT

3.4 Manpower Management in Police Department

Police Department is the biggest Government Department in the State giving employment to more than twenty thousand people. The performance review of "Manpower Management in Police Department' revealed gross irregularities in recruitment, promotion, training, deployment of police personnel and their performance appraisal.